PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-057662
(43)Date of publication of application : 22.02.2002

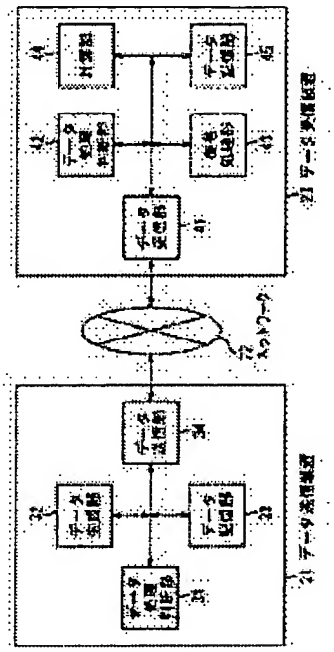
(51)Int.Cl. H04L 9/10
H04L 9/14

(21)Application number : 2000-238815
(22)Date of filing : 07.08.2000

(71)Applicant : SONY CORP
(72)Inventor : MUTO AKIHIRO

(54) INFORMATION-PROCESSING DEVICE AND METHOD, AND RECORD MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To secure a processing capacity for decoding coded contents data.
SOLUTION: A data reception device 23 for receiving contents data transmitted from a data transmission device 21 for decoding processing confums the details of meta data where information regarding the coding of the contents data is described. When a plurality of data processings are requested by a decoding processing part 43, the decoding processing part 43 selects top priority processing from each processing order being set to the meta data, and performs processing from the top priority processing. The decoding processing part 43 calculates time required for other processing, and judges whether other processing can be made or not until the data unit of the contents data requiring the next top priority processing is transmitted from a data processing judgment part 42. The decoding processing part 43 performs processing when it judges that other processing can be made, and confirms the handling information of other processing being set to the meta data when other processing cannot be made, and performs processing based on the handling information.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－57662
（P2002－57662A）
(43)公開日　平成14年２月22日(2002.2.22)

(51)Int.Cl.'	識別記号	FI	テーマコード'（参考）
H04L 9/10 9/14		H04L 9/00	621Z 5J104 641

審査請求　未請求　請求項の数4　ＯＬ　（全 26 頁）

(21)出願番号　特願2000－238815(P2000－238815)

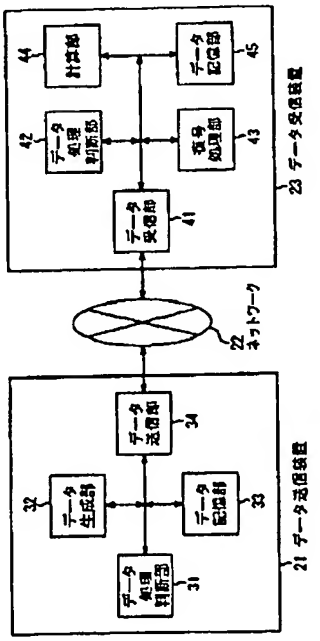
(22)出願日　平成12年８月７日(2000.8.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　武藤　明宏
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5J104 AA01 AA32 DA04 JA13 JA28
PA07 PA10

(54)【発明の名称】　情報処理装置、情報処理方法、並びに記録媒体

(57)【要約】
【課題】　暗号化されたコンテンツデータを復号する処理能力を確保する。
【解決手段】　データ送信装置２１から送信されるコンテンツデータを受信して復号処理するデータ受信装置２３は、コンテンツデータを処理する前に、コンテンツデータの暗号化に関する情報が記述されているメタデータの内容を確認する。複数のデータ処理が復号処理部４３に要求されている場合、復号処理部４３は、メタデータにより設定されているそれぞれの処理順位から、最優先処理を選択し、最優先処理から処理を行う。復号処理部４３は、他の処理に要する時間を算出し、次の最優先処理が必要なコンテンツデータのデータ単位が、データ処理判断部４２から転送されてくるまでの間に、他の処理を行うことが可能であるか否かを判定する。復号処理部４３は、他の処理を行うことが可能と判定した場合、処理を行い、不可能と判定した場合、メタデータに設定されている他の処理の取扱情報を確認し、取扱情報に基づいて処理する。



【特許請求の範囲】
【請求項１】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、
前記受信手段により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識手段と、
前記第１の認識手段により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータの他の処理に優先して処理する第１の処理手段とを含むことを特徴とする情報処理装置。
【請求項２】　前記他の処理に要する時間を算出する算出手段と、
第１の前記優先処理が必要な前記コンテンツデータの処理が終了されている場合、第２の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間と、前記算出手段により算出された前記他の処理に要する時間を比較する比較手段と、
前記比較手段による比較の結果、前記第２の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間が、前記他の処理に要する時間より長いと判定された場合、前記他の処理を処理する第２の処理手段と、
前記比較手段による比較の結果、前記第２の前記優先処理が必要な前記コンテンツデータの処理が開始されるまでの時間が、前記他の処理に要する時間より短いと判定された場合、前記他の処理の取扱方法を認識する第２の認識手段と、
前記第２の認識手段により認識された取扱方法に基づいて前記他の処理を処理する第３の処理手段とをさらに含むことを特徴とする請求項１に記載の情報処理装置。
【請求項３】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、
前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識ステップと、
前記第１の認識ステップの処理により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータの他の処理に優先して処理する第１の処理ステップとを含むことを特徴とする情報処理方法。
【請求項４】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、
前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識ステップと、
前記第１の認識ステップの処理により認識された前記処理順位が上位にある優先処理を、前記コンテンツデータの他の処理に優先して処理する第１の処理ステップとを含むことを特徴とするコンピュータが読みとり可能なプログラムが格納されている記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理装置および情報処理方法、並びに記録媒体に関し、特に、要求されるデータ処理毎に設定されている処理順位を認識し、処理順位が上位にあるデータ処理を優先的に処理することにより、システム毎に設計したハードウエアを用いることなく、迅速にデータを処理することができるようにした情報処理装置および情報処理方法、並びに記録媒体に関する。
【０００２】
【従来の技術】近年、コンテンツデータをネットワークを介して配信する配信システムが構築されている。配信されるコンテンツデータは、データの改竄を防ぐため、暗号化や、ディジタル署名を付加するなどの処理が施されている。暗号化されたコンテンツデータは、利用者の端末により復号処理され、利用者はそれを利用することができる。
【０００３】暗号化技術の安全性は、復号する際の処理の難しさに依存しているため、暗号化技術の高度化にともなって、コンテンツデータを利用する利用者の端末には、より処理能力の高い端末が要求されるようになっている。
【０００４】そこで、処理能力を確保するために、利用者端末に復号処理専用のLSI（LargeScale Integration）を配置することが考えられる。図１は、復号処理専用のLSI（以下、復号LSIと称する）の構成例を示している。
【０００５】復号LSI１は、復号LSI１の外部に配置されるコントロールマイクロコンピュータ（以下、コントロールマイコンと略称する）２から転送される指令により復号処理を行う。復号処理には、暗号化されたコンテンツデータを復号する処理の他に、コンテンツデータに付加されているディジタル署名を検証する処理が含まれる。復号LSI１が処理した結果は、復号LSI１の外部に配置される外部メモリ３に記憶される。
【０００６】復号LSI１は、通信インタフェース１１、コントロールユニット１２、RAM（Random Access Memory）１３、メモリコントローラ１４、フラッシュメモリ１５、べき乗演算器１６、ハッシュ値演算器１７から構成される。
【０００７】コントロールマイコン２から転送される指令は、通信インタフェース１１を介してコントロールユニット１２に伝えられる。コントロールユニット１２は、べき乗演算器１６およびハッシュ値演算器１７などを補助的に用いつつ、復号LSI１の全体の動作を制御し、暗号化されているデータの復号処理、およびディジ

タル署名の検証処理などを行う。

【０００８】RAM１３には、コントロールユニット１２が利用するプログラムが記憶されている。

【０００９】メモリコントローラ１４は、外部メモリ３に対するデータの読み書きを制御する。

【００１０】フラッシュメモリ１５には、コントロールユニット１２の指令によりべき乗演算器１６、およびハッシュ値演算器１７が演算した結果や、処理に必要なデータが、適宜、記憶される。

【００１１】利用者が使用する端末に、上述したような復号LSI１を配置することにより、コンテンツデータの復号処理能力を確保することが可能となる。

【００１２】

【発明が解決しようとする課題】しかしながら、利用者端末に復号LSI１（ハードウエア）を設置する場合、暗号化されたコンテンツデータの復号処理能力は、暗号化のセキュリティレベルに応じて計算量が異なるため、最大の負荷を処理することができるように復号LSI１を構成する必要がある。その結果、コスト高となる課題があった。また、処理能力を変更する必要が生じた場合、LSIを設計し直す必要があるため、バージョンアップ等の変更が実質的に困難になる課題があった。

【００１３】本発明はこのような状況に鑑みてなされたものであり、暗号化されたコンテンツデータを利用者端末において復号する場合に、システム毎に設計したハードウエアを利用することなく、低コストで、かつ、比較的容易に機能を変更できるシステムを実現できるようにするものである。

【００１４】

【課題を解決するための手段】本発明の情報処理装置は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、受信手段により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識手段と、第１の認識手段により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第１の処理手段とを含むことを特徴とする。

【００１５】本発明の情報処理装置は、他の処理に要する時間を算出する算出手段と、第１の優先処理が必要なコンテンツデータの処理が終了されている場合、第２の優先処理が必要なコンテンツデータの処理が開始されるまでの時間と、算出手段により算出された他の処理に要する時間を比較する比較手段と、比較手段による比較の結果、第２の優先処理が必要なコンテンツデータの処理が開始されるまでの時間が、他の処理に要する時間より長いと判定された場合、他の処理を処理する第２の処理手段と、比較手段による比較の結果、第２の優先処理が必要なコンテンツデータの処理が開始されるまでの時間が、他の処理に要する時間より短いと判定された場合、他の処理の取扱方法を認識する第２の認識手段と、第２の認識手段により認識された取扱方法に基づいて他の処理を処理する第３の処理手段とをさらに含むようにすることができる。

【００１６】本発明の情報処理方法は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識ステップと、第１の認識ステップの処理により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第１の処理ステップとを含むことを特徴とする。

【００１７】本発明の記録媒体のプログラムは、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識する第１の認識ステップと、第１の認識ステップの処理により認識された処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理する第１の処理ステップとを含むことを特徴とする。

【００１８】本発明の情報処理装置、情報処理方法、および記録媒体においては、コンテンツデータと、その特徴に関する情報が記述されている特徴情報が受信され、受信された特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位が認識される。処理順位が上位にある優先処理は、コンテンツデータの他の処理に優先して処理される。

【００１９】

【発明の実施の形態】図２は、本発明を適用したデータ処理システムの構成例を示すブロック図である。データ送信装置２１により生成され、暗号化されたコンテンツデータは、ネットワーク２２を介してデータ受信装置２３に送信される。

【００２０】データ送信装置２１は、データ処理判断部３１、データ生成部３２、データ記憶部３３、およびデータ送信部３４から構成される。

【００２１】データ処理判断部３１は、データ送信装置２１の全体の動作を制御する。データ生成部３２は、所定の方法により提供されたコンテンツデータを暗号化したり、ディジタル署名を生成する（以下、コンテンツデータの暗号化処理、およびディジタル署名の生成処理をまとめて暗号関連処理と称する）。また、データ生成部３２は、コンテンツデータの暗号化に関するデータなどが記述されているメタデータを生成する。データ記憶部３３は、データ生成部３２により生成されたコンテンツデータおよびメタデータを記憶する。データ送信部３４は、データ受信装置２３からの要求に応じて、データ記憶部３３に記憶されているメタデータおよびコンテンツ

データを送信する。

【００２２】ネットワーク２２は、データ送信装置２１およびデータ受信装置２３の間で送受信されるデータの伝送路であり、例えば、インターネット、電話回線網、ケーブルテレビジョン放送網、衛星を介したディジタルテレビジョン放送網等により構成される。

【００２３】データ受信装置２３は、データ受信部４１、データ処理判断部４２、復号処理部４３、計算部４４、およびデータ記憶部４５より構成される。

【００２４】データ受信部４１は、データ送信装置２１から送信されたメタデータおよびコンテンツデータを受信する。データ処理判断部４２は、データ受信装置２３の全体の動作を制御する。復号処理部４３は、データ受信部４１により受信されたコンテンツデータが暗号化されている場合にはコンテンツデータを復号し、ディジタル署名が付加されている場合には、ディジタル署名の検証などの処理を行う（以下、コンテンツデータの復号処理、およびディジタル署名の検証処理をまとめて復号関連処理と称する）。計算部４４は、データ処理判断部４２の指令を受けて、演算処理機能を提供する。データ記憶部４５は、データ受信部４１により受信されたコンテンツデータ、および復号処理部４３により復号され、かつディジタル署名が検証されたコンテンツデータを記憶する。

【００２５】次に、データ送信装置２１が送信するメタデータおよびコンテンツデータを、データ受信装置２３が受信し、処理する一連の処理について、図３乃至図５のフローチャートを参照して説明する。

【００２６】図３は、データ送信装置２１の処理を説明するフローチャートである。ステップS１において、データ生成部３２は、外部から所定の方法により提供されるアナログデータまたはディジタルデータを取得し、コンテンツデータを作成する。データ生成部３２は、ネットワーク２２を介してデータ受信装置２３に対して送信することが可能な形式に圧縮し、暗号関連処理を施して、コンテンツデータを作成する。

【００２７】また、データ生成部３２は、メタデータを生成する。メタデータには、送信されるコンテンツデータの特徴、コンテンツデータの暗号関連処理に関する情報である暗号関連情報、およびデータ受信装置２３がコンテンツデータを処理するために必要な情報が記述される。コンテンツデータの特徴には、例えば、コンテンツデータの制作者、制作時期、制作者を識別する制作者ID、コンテンツデータの利用形態、コンテンツデータ利用形態毎の料金、コンテンツデータの再生時間、コンテンツデータの圧縮方法、総データ量、データの転送速度などが含まれる。また、コンテンツデータの暗号関連情報には、例えば、暗号化アルゴリズム、ディジタル署名の生成アルゴリズム、データ単位が含まれる。さらに、データ受信装置２３がコンテンツデータを処理するために必要な情報には、コンテンツデータの処理の種類、コンテンツデータの転送周期、処理順位、および取扱情報が含まれる。これらの具体例については後述する。

【００２８】ステップS２において、データ記憶部３３は、ステップS１の処理でデータ生成部３２により作成されたコンテンツデータおよびメタデータを記憶する。

【００２９】ステップS３において、データ処理判断部３１は、データ受信装置２３からメタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。データ処理判断部３１によりメタデータの送信が要求されたと判定された場合、処理はステップS４に進む。

【００３０】ステップS４において、データ送信部３４は、データ記憶部３３に記憶されているメタデータを、ネットワーク２２を介してデータ受信装置２３に送信する。後述するように、メタデータを受信したデータ受信装置２３は、メタデータに記述されている情報を分析し、コンテンツデータの処理を準備する。メタデータに記述されているコンテンツデータの情報に応じて、コンテンツデータを処理する準備が完了した場合、データ受信装置２３は、コンテンツデータの送信をデータ送信装置２１に要求する。

【００３１】そこで、ステップS５において、データ処理判断部３１は、データ受信装置２３からコンテンツデータの送信が要求されたか否かを判定する。

【００３２】ステップS５において、データ処理判断部３１によりデータ受信装置２３からコンテンツデータの送信が要求されていないと判定された場合、データ処理判断部３１は、データ受信装置２３が、コンテンツデータの処理の準備が完了していないと認識し、コンテンツデータの送信が要求されるまで待機する。

【００３３】ステップS５において、データ処理判断部３１が、データ受信装置２３からコンテンツデータの送信が要求されたと判定した場合、処理はステップS６に進み、データ送信部３４は、データ記憶部３３に記憶されているコンテンツデータを、ネットワーク２２を介してデータ受信装置２３に対して送信する。

【００３４】図４および図５は、データ受信装置２３の処理を説明するフローチャートである。ステップS１１において、データ処理判断部４２は、データ受信装置２３を管理する利用者からコンテンツデータの受信の指令が入力された場合、データ送信装置２１に対して、そのコンテンツデータに対応するメタデータの送信を要求する。

【００３５】ステップS１２において、データ受信部４１は、データ送信装置２１から送信されたメタデータを、ネットワーク２２を介して受信する。データ受信部４１が受信したメタデータは、データ処理判断部４２に転送され、データ処理判断部４２により記述されている内容が分析される。データ処理判断部４２は、コンテン

ツデータは暗号関連処理が施されていると認識し、メタデータを復号処理部４３に転送する。

【００３６】ステップＳ１３において、復号処理部４３は、メタデータに記述されている内容を分析し、全ての復号関連処理を抽出する。

【００３７】ステップＳ１４において、復号処理部４３は、メタデータを参照して、ステップＳ１３で抽出された復号関連処理から、データ処理判断部４２が復号処理部４３に対して処理を要求するタイミング（データ処理部４２が復号処理部４３に対してコンテンツデータを転送するタイミング）に周期性がある処理をさらに抽出する。

【００３８】ステップＳ１５において、ステップＳ１４の処理で抽出した処理から、メタデータに予め設定されているそれぞれの処理の優先度を示す処理順位を確認し、処理順位が最上位にある復号関連処理を最優先処理として選択する。

【００３９】ステップＳ１６において、復号処理部４３は、最優先処理が必要なコンテンツデータの転送周期を基準周期として設定する。

【００４０】ステップＳ１７において、復号処理部４３から、最優先処理を選択し、基準周期を設定した旨の通知を受けたデータ処理判断部４２は、データ送信装置２１に対してコンテンツデータの送信を要求する。

【００４１】ステップＳ１８において、データ受信部４１は、データ送信装置２１が送信したコンテンツデータを、ネットワーク２２を介して受信する。

【００４２】データ受信装置４１からコンテンツデータを受け取ったデータ処理判断部４２は、復号関連処理が必要なコンテンツデータ単位を復号処理部４３に転送する前に、ステップＳ１９の判定処理を行う。ステップＳ１９において、データ処理判断部４２は、復号関連処理が必要なコンテンツデータの処理が終了したか否かを判定する。処理開始時においては、復号関連処理が必要なコンテンツデータがまだ存在しているため、処理は終了することができないと判定され、ステップＳ２０に進む。

【００４３】ステップＳ２０において、データ処理判断部４２は、復号処理部４３に対して復号関連処理が必要なコンテンツデータ単位を転送する。転送されるコンテンツデータ単位は、ステップＳ１６で設定した基準周期に基づいて、最優先処理が必要なコンテンツデータ単位から転送される。復号処理部４３により復号関連処理が施されたコンテンツデータ単位は、データ記憶部４５に、適宜、記憶される。以下、図６を参照してデータ処理判断部４２が転送するコンテンツデータ単位について説明する。

【００４４】最優先処理データ単位１がデータ処理判断部４２から転送される時間を時間０として、ステップＳ１６の処理で設定した基準周期毎に最優先処理データ単位が転送される。図６では、基準周期毎に最優先処理データ単位２、最優先処理データ単位３、および最優先処理が必要なコンテンツデータ単位の最後のコンテンツデータ単位である最優先処理データ単位nが転送されている。また、最優先処理データ単位nの後には後述する遅延処理データが転送されている。

【００４５】タイム１、およびタイム２は基準周期の時間の長さを示しており、タイム１、およびタイム２はそれぞれ、タイム１－１、タイム２－１、およびタイム１－２、タイム２－２に分かれている。

【００４６】タイム１－１、タイム２－１、タイムn－１はそれぞれ最優先処理データ単位１、最優先処理データ単位２、および最優先処理データ単位nを、復号処理部４３が復号関連処理する際に要する時間である。

【００４７】タイム１－２、タイム２－２はそれぞれ復号処理部４３が最優先処理データ単位１、または最優先処理データ単位２の復号関連処理を終了し、次のコンテンツデータ単位が転送されるのを待機している時間である。本発明では、タイム１－２、タイム２－２において、復号処理部４３は、最優先処理以外の他の復号関連処理が実行可能であるか否かを判断するが、その処理については後述する。

【００４８】ステップＳ２１において、復号処理部４３は、データ処理判断部４２から転送された最優先処理が必要なコンテンツデータ単位の処理を行う。すなわち、復号処理部４３は、最優先処理データ単位１を受信した場合、処理を開始する。

【００４９】ステップＳ２２において、復号処理部４３は、最優先処理以外の復号関連処理が必要なコンテンツデータ単位（以下、単に、他のコンテンツデータ単位と称する）が、データ処理判断部４２から転送されてきたか否かを判定する。復号処理部４３が、他のコンテンツデータ単位が転送されてきたと判定するまでステップＳ１９乃至ステップＳ２１の処理は繰り返される。

【００５０】ステップＳ２２において、復号処理部４３は、他のコンテンツデータ単位がデータ処理判断部４２から転送されてきたと判定した場合、処理はステップＳ２３に進む。

【００５１】ステップＳ２３において、復号処理部４３は、図６の最優先処理データ単位１の処理を終了しており、最優先処理データ単位２がデータ処理判断部４２から転送されてくるのを待機している状態の場合（タイム１－２の状態の場合）、データ処理判断部４２から転送されてきた他のコンテンツデータ単位の復号関連処理に要する時間を算出する。データ処理判断部４２から転送されてきた他のコンテンツデータ単位が複数ある場合、復号処理部４３は、ステップＳ１５で認識した復号関連処理の処理順位を確認し、転送されてきているコンテンツデータ単位に必要な復号関連処理のうちの最も処理順位が高い処理に要する時間を算出する。なお、復号処理部４３は、最優先処理を実行している場合（タイム１－

1の状態の場合）、データ処理判断部４２から転送されてくる他のコンテンツデータ単位を無視して最優先処理を続行する。

【００５２】ステップS２４において、復号処理部４３は、ステップS２３で算出した他のコンテンツデータ単位の処理に要する時間から、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理が可能か否かを判定する。すなわち、復号処理部４３は、タイム１－２の間に、他のコンテンツデータ単位の処理を完了することが可能か否かを判定する。

【００５３】ステップS２４において、復号処理部４３は、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理を完了することは可能と判定した場合、処理はステップS２５に進み、復号処理部４３は、他のコンテンツデータ単位の復号関連処理を行う。その後、処理はステップS２２の処理に戻り；以降の処理が繰り返し実行される（復号関連処理が必要なコンテンツデータが存在する場合、その処理毎に、処理順位に基づいてステップS２３以降で順次、処理されることとなる）。

【００５４】ステップS２４において、復号処理部４３は、最優先処理が実行されていない時間に、他のコンテンツデータ単位の処理を完了することは不可能と判定した場合（タイム１－２の時間内に、処理が完了しないと判定した場合）、ステップS２６において、復号処理部４３は、他のコンテンツデータ単位の処理方法をメタデータに記述されている取扱情報から認識する。

【００５５】取扱情報には、他のコンテンツデータ単位の処理方法が設定されており、データ送信装置２１で設定されてメタデータに記述される。

【００５６】取扱情報に記述されている他のコンテンツデータ単位の処理方法には、例えば次のような方法がある。処理方法１は、復号処理部４３は、最優先処理が全て終了した後に、他のコンテンツデータ単位の処理を開始する処理方法（遅延処理）である。この場合、復号処理部４３は、他のコンテンツデータ単位を遅延処理することをデータ処理判断部４２に通知する。

【００５７】処理方法２は、復号処理部４３は、他のコンテンツデータ単位の処理を実行せずに、他のコンテンツデータ単位の処理を実行しないことをデータ処理判断部４２に通知のみする処理方法である。

【００５８】処理方法３は、復号処理部４３は、他のコンテンツデータ単位の処理を実行しないだけでなく、他のコンテンツデータ単位の処理を実行しないことをデータ処理判断部４２に通知もしない処理方法であり、復号処理部４３は、他のコンテンツデータ単位が転送されてきたとしても、他のコンテンツデータ単位を無視して最優先処理を続行する。

【００５９】ステップS２６において、復号処理部４３は、取扱情報に処理方法１が設定されていると認識した場合、ステップS２７に進み、復号処理部４３は、他のコンテンツデータ単位を遅延処理することを決定する。また、復号処理部４３は、他のコンテンツデータ単位を遅延処理することをデータ処理判断部４２に通知する。その後、処理はステップS１９に戻り、同様の処理が繰り返し実行される。最優先処理が全て終了した場合、復号処理部４３は、図６のようにデータ処理判断部４２から転送される遅延処理データ単位の復号関連処理を実行する。

【００６０】ステップS２６において、復号処理部４３は、取扱情報に処理方法２が設定されていると認識した場合、ステップS２８に進み、復号処理部４３は、他のコンテンツデータ単位を処理せずに、データ処理判断部４２に他のコンテンツデータを処理しないことを通知する。その後、処理はステップS１９に戻り、同様の処理が繰り返し実行される。

【００６１】ステップS２６において、復号処理部４３は、取扱情報に処理方法３が設定されていると認識した場合、ステップS２９に進み、復号処理部４３は、他のコンテンツデータ単位を処理しないだけでなく、データ処理判断部４２になにも通知しない。その後、処理はステップS１９に戻り、同様の処理が繰り返し実行される。

【００６２】ステップS１９において、復号処理部４３が復号関連処理は全て終了したと判定した場合、処理は終了される。

【００６３】なお、取扱情報は、データ送信装置２１において設定され、メタデータに記述されるとしたが、データ処理判断部４２に取扱情報を予め与えておき、データ処理判断部４２は、他のコンテンツデータ単位を認識した場合、与えられた取扱情報に基づいて処理を行うことが可能である。

【００６４】また、復号処理部４３が最優先処理を実行している場合でも、さらに処理順位が上位にある処理が新しくデータ送信装置２１から送信され、データ処理判断部４２から復号処理部４３に転送された場合、復号処理部４３は、最優先処理を中止し、新しく転送されたコンテンツデータを処理するように取扱情報に設定することも可能である。

【００６５】図７は、本発明を適用したコンテンツ配信システムの構成を示す図である。コンテンツプロバイダ５１は、コンテンツサーバ５２を管理しており、コンテンツデータおよびメタデータを作成する。コンテンツプロバイダ５１が作成したコンテンツデータおよびメタデータは、サービスプロバイダ５３が管理するサービスサーバ５４に供給される。コンテンツデータは、映画、音楽などのディジタルデータであり、メタデータにはそれらのデータに関する情報が記述される。

【００６６】サービスプロバイダ５３は、ネットワーク２２を介して、契約者である利用者５５に対してコンテ

ンツデータおよびメタデータを送信する。

【００６７】利用者５５は、サービスプロバイダ５３から送信されたコンテンツデータおよびメタデータを、自らが操作する利用者端末５６において利用する。

【００６８】決済センタ５７は、決済サーバ５８を管理しており、利用者５５に対してコンテンツデータの使用権情報を発行するとともに、使用権情報の代金の決済処理を行う。また、決済センタ５７は、利用者５５から支払われた代金を、コンテンツプロバイダ５１と、サービスプロバイダ５３の間で予め設定された契約に基づいて分配する。

【００６９】図8は、コンテンツサーバ５２の構成例を示すブロック図である。コンテンツサーバ５２は、データキャプチャ装置７１、データ編集装置７２、メタデータ生成装置７３、データ暗号化装置７４、データ記憶装置７５、およびデータ送信装置７６より構成される。

【００７０】データキャプチャ装置７１は、外部から取り込んだデータを、コンテンツサーバ５２の各装置が処理できるデータ形式に変換する。

【００７１】データ編集装置７２は、データキャプチャ装置７１から転送されたデータから、利用者５５に提供するコンテンツデータを作成する装置である。また、データ編集装置７２は、メタデータ生成装置７３が生成したメタデータをコンテンツデータに付加する。

【００７２】データ暗号化装置７４は、データ編集装置７２から転送されたコンテンツデータおよびメタデータに暗号関連処理を施す。

【００７３】データ記憶装置７５は、データ暗号化装置７４により暗号関連処理が施されたメタデータおよびコンテンツデータを記憶し、必要に応じてデータ送信装置７６に転送する。

【００７４】データ送信装置７６は、サービスプロバイダ５３が管理するサービスサーバ５４にコンテンツデータおよびメタデータを送信する。なお、具体的な各装置の処理については、図１６のフローチャートを参照して後述する。

【００７５】図9は、データ暗号化装置７４の詳細な構成例を示すブロック図である。データ暗号化装置７４は、入出力インタフェースブロック９１、データ処理判断ブロック９２、データ記憶ブロック９３、乱数生成ブロック９４、および暗号化処理ブロック９５から構成される。さらに、暗号化処理ブロック９５は、暗号化処理サブブロック９６、ディジタル署名生成サブブロック９７、およびハッシュ値計算サブブロック９８より構成される。

【００７６】入出力インタフェースブロック９１は、データ編集装置７２から供給されるメタデータおよびコンテンツデータを、データ処理判断ブロック９２に転送する。

【００７７】データ処理判断ブロック９２は、データ暗号化装置７４の全体の動作を制御する。

【００７８】データ記憶ブロック９３は、暗号化処理ブロック９５において、暗号関連処理が施されたメタデータおよびコンテンツデータや、処理に必要なデータを、適宜、記憶する。

【００７９】乱数生成ブロック９４は、データ処理判断ブロック９２からの指令により乱数を生成し、暗号化処理ブロック９５に供給する。乱数生成ブロック９４が生成する乱数は、暗号化アルゴリズムであるDES (Data Encryption Standard) 、RSA (Rivest-Shamir-Adleman scheme) などの共通鍵暗号方式で暗号関連処理する場合の鍵として利用される。

【００８０】暗号化処理ブロック９５は、コンテンツの暗号化およびディジタル署名の生成処理を行う。この暗号化処理ブロック９５の暗号化処理サブブロック９６は、DES、RSAなどの暗号化アルゴリズムによりコンテンツデータの暗号化処理を行う。

【００８１】ディジタル署名生成サブブロック９７は、DSA (Digital Signature Algorithm) などによるディジタル署名の生成アルゴリズムによりディジタル署名を生成する。ディジタル署名は、データの改竄のチェックおよびデータの制作者を認証するためのデータである。

【００８２】ハッシュ値計算サブブロック９８は、ハッシュ関数による計算を行う。ハッシュ関数は、送信するデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、出力であるハッシュ値から入力データを復元することが難しく、また、同一の出力結果のハッシュ値を持つ入力データを探し出すことが困難である（一方向である）特徴を有する。

【００８３】ここで、ディジタル署名の生成および検証について説明する。ディジタル署名の生成者は、送信するデータから特定のアルゴリズムを用いて、メッセージダイジェストを作成する（ハッシュ値計算サブブロック９８により、送信するデータに、ハッシュ関数を適用し、メッセージダイジェストを作成する）。ディジタル署名の生成者は、自分の秘密鍵（乱数生成ブロック９４により生成された乱数）を使って、このメッセージダイジェストと送信するデータの全文を暗号化し、利用者に送信する。

【００８４】一方、データの利用者は、データを受信し、ディジタル署名の生成者が提供する公開鍵を利用して、暗号化されているデータの全文、およびメッセージダイジェストを復号する。次に、データの利用者は復号したデータの全文から、ディジタル署名の生成者と同一の方式（同一のハッシュ関数）でメッセージダイジェストを作成する。生成されたメッセージダイジェストと受信されたメッセージダイジェストを比較することにより、ディジタル署名の検証が行なわれる。すなわち、データの送信者から送信され、受信者が復号したメッセー

ジダイジェストと、受信者が復号したデータの全文から、送信者と同一の方式により作成したメッセージダイジェストが等しければ、そのデータは改竄などの不正な処理が行われていないことを表す。

【００８５】なお、データ暗号化装置７４において、説明の便宜上、暗号化処理サブブロック９６、およびディジタル署名生成サブブロック９７は暗号関連処理を行うことが可能であるとしたが、通常は、復号関連処理も行うことが可能である。すなわち、暗号化処理サブブロック９６はデータの暗号化および復号が可能であるし、ディジタル署名生成サブブロック９７はディジタル署名の生成および検証が可能である。

【００８６】さらに、後述する図１４の暗号化処理ブロック１６３に配置されている暗号化処理部１８６を構成するサブブロックも、データ暗号化装置７４を構成するサブブロックと同様に、復号関連処理だけでなく暗号関連処理を実行することができる。また、サービスサーバ５４に配置されているデータ暗号化装置１１４も上述したコンテンツサーバ５２に配置されているデータ暗号化装置７４、および暗号化処理ブロック１６３と同様に、復号関連処理だけでなく暗号関連処理を実行することができる。これにより、それぞれの装置間で送受信されるデータに、改竄などの不正な処理が行われることを防ぐことが可能となる。

【００８７】上述したような暗号関連処理が施されたコンテンツデータおよびメタデータは、サービスプロバイダ５３が管理するサービスサーバ５４に送信される。

【００８８】図１０は、サービスサーバ５４の構成例を示すブロック図である。サービスサーバ５４は、データ送受信装置１１１、データ編集装置１１２、メタデータ生成装置１１３、データ暗号化装置１１４、コンテンツプロモーションサーバ１１５、およびデータ記憶装置１１６より構成される。

【００８９】データ送受信装置１１１は、コンテンツサーバ５２から送信されるコンテンツデータおよびメタデータを受信する。また、データ送受信装置１１１は、利用者端末５６に対し、ネットワーク２２を介してコンテンツデータおよびメタデータを送信する。データ送受信装置１１１は、コンテンツデータおよびメタデータを送信するタイミングを判断する。送信するタイミングは、例えば、利用者５５からの要求に応じて送信する場合や、メタデータに記述されているタイミングで送信する場合などがある。

【００９０】データ編集装置１１２は、サービスサーバ５４の各装置で処理されたデータを編集し、利用者５５に提供する形態にデータを編集する。

【００９１】メタデータ生成装置１１３は、メタデータを生成する。メタデータ生成装置１１３が生成するメタデータには、サービスプロバイダ５３がコンテンツデータを利用者５５に提供する際に、サービスプロバイダ５３が利用者５５に対して通知する情報が記述される。

【００９２】データ暗号化装置１１４は、メタデータ生成装置１１３が生成したメタデータにディジタル署名を生成するなどの暗号関連処理を行う。データ暗号化装置１１４の詳細な構成は、図８に示すコンテンツサーバ５２のデータ暗号化装置７４（図９）の構成と同様である。

【００９３】コンテンツプロモーションサーバ１１５は、サービスプロバイダ５３が利用者５５に提供するコンテンツの一覧情報を作成するとともに、ディスカウント情報などを利用者５５の要求に応じて提供する。コンテンツプロモーションサーバ１１５は、WWWサーバとして設置され、利用者５５は利用者端末５６に装備されているブラウザを利用することにより、コンテンツプロモーションサーバ１１５が提供するサービスを受けることができる。さらに、コンテンツプロモーションサーバ１１５は、利用者５５からの電話による問い合わせに対応できるようにもなっている。

【００９４】データ記憶装置１１６は、データ編集装置１１２で編集されたデータを記憶し、利用者５５からの要求に応じて、データ送受信装置１１１に対してコンテンツデータおよびメタデータを転送する。なお、具体的な各装置の処理については、図１９のフローチャートを参照して後述する。

【００９５】図１１は、決済センタ５７が管理している決済サーバ５８の構成例を示すブロック図である。決済サーバ５８は、データ送受信装置１３１、ライセンス装置１３２、ユーザ管理装置１３３、著作権管理装置１３４、課金装置１３５、および決済装置１３６より構成される。

【００９６】データ送受信装置１３１は、利用者端末５６から、ネットワーク２２を介して通知されるコンテンツデータの使用権の購入要求情報を受信するとともに、コンテンツプロバイダ５１およびサービスプロバイダ５３に対して、利用者５５から回収した代金の課金情報を送信する。

【００９７】ライセンス装置１３２は、利用者５５からコンテンツデータの使用権購入が要求された場合、使用権情報の発行処理を行う。

【００９８】ユーザ管理装置１３３は、サービスプロバイダ５３から、コンテンツデータの提供を受ける契約をしている利用者５５、およびその利用者５５が操作する利用者端末５６の情報を管理する。利用者５５および利用者端末５６の情報には、利用者端末５６に含まれるセットトップボックスの契約日、契約条件、サービスの利用情報などが含まれる。

【００９９】著作権管理装置１３４は、コンテンツデータの著作権の他、サービスプロバイダ５３から提供される利用者５５が利用可能なコンテンツデータの利用形態、および利用者５５によるコンテンツデータの購入履

歴などを管理する。

【０１００】課金装置１３５は、コンテンツデータの使用権情報の料金情報を管理するとともに、利用者５５に対して、課金情報を通知する。

【０１０１】決済装置１３６は、課金装置１３５から決済処理の要求をうけて、決済処理を行う。具体的な決済方法には、クレジットカードによる決済方法、プリペイド型の電子マネーによる決済方法が含まれる。なお、決済サーバ５８の使用権情報の発行処理については、図２１および２２のフローチャートを参照して後述する。

【０１０２】図１２は、利用者５５が管理する利用者端末５６の構成例を示すブロック図である。利用者端末５６は、セットトップボックス１５１（以下、適宜、STB１５１と称する）、およびデータ再生装置１５２より構成される。

【０１０３】STB１５１は、ネットワーク２２を介して、サービスサーバ５４、および決済サーバ５８との間でデータの送受信を行う。STB１５１の詳細な構成例は図１３に示す。

【０１０４】データ再生装置１５２は、サービスサーバ５４から提供され、STB１５１が処理したコンテンツデータを再生する装置である。データ再生装置１５２は、例えば、テレビジョン受像機、パーソナルコンピュータなどの電子機器により構成される。

【０１０５】図１３は、セットトップボックス１５１の構成例を示すブロック図である。STB１５１は、データ送受信ブロック１６１、コントローラ１６２、暗号化処理ブロック１６３、フラッシュメモリ１６４、および外部RAM（Random Access Memory）１６５から構成される。

【０１０６】データ送受信ブロック１６１は、サービスサーバ５４から、ネットワーク２２を介して送信されるコンテンツデータおよびメタデータ、若しくは決済サーバ５８から送信されるコンテンツデータの使用権情報などを受信する。また、データ送受信ブロック１６１は、サービスサーバ５４に対するデータの送信要求、および決済サーバ５８に対する使用権情報を要求する情報などを送信するとともに、データ再生装置１５２に、処理結果を転送する。

【０１０７】コントローラ１６２は、ソフトウエアにより制御され、STB１５１全体の動作を制御する。

【０１０８】暗号化処理ブロック１６３は、データ送受信ブロック１６１が受信するコンテンツデータおよびメタデータの復号関連処理を行う。詳細な構成例については図１４に示す。

【０１０９】フラッシュメモリ１６４は、STB１５１の電源遮断後もデータを記憶している不揮発性のメモリである。フラッシュメモリ１６４には、各ブロックが処理するために必要なデータ、および各ブロックの処理結果が、適宜、記憶される。

【０１１０】外部RAM１６５は、暗号化処理ブロック１６３による処理結果、システム制御データ、および課金処理結果等を記憶する。

【０１１１】図１４は、暗号化処理ブロック１６３の詳細な構成例を示すブロック図である。暗号化処理ブロック１６３は、入出力インタフェースブロック１８１、マイクロプロセッサ１８２、RAM１８３、乱数生成ブロック１８４、フラッシュメモリ１８５、および暗号化処理部１８６より構成される。さらに、暗号化処理部１８６は、暗号化処理サブブロック１８７、ディジタル署名検証サブブロック１８８、およびハッシュ値計算サブブロック１８９より構成される。

【０１１２】入出力インタフェースブロック１８１は、データ送受信ブロック１６１が受信したコンテンツデータおよびメタデータのうち、コントローラ１６２により復号関連処理が必要であると判断され、暗号化処理ブロック１６３に転送されるデータを受信する。入出力インタフェースブロック１８１は、コントローラ１６１から供給されるデータを、マイクロプロセッサ１８２に転送する。マイクロプロセッサ１８２は、暗号化処理ブロック１６３の全体の動作を制御する。

【０１１３】RAM１８３は、マイクロプロセッサ１８２が処理をするのに必要なプログラムを記憶している。また、RAM１８３には、マイクロプロセッサ１８２が処理した結果が記憶される。

【０１１４】乱数生成ブロック１８４は、マイクロプロセッサ１８２からの指令により乱数を生成し、暗号化処理部１８６に供給する。乱数生成ブロック１８４が生成した乱数は、DES、RSAなどの共通鍵暗号方式で暗号関連処理が施されたデータを、復号する場合の鍵として利用される。

【０１１５】フラッシュメモリ１８５は、不揮発性のメモリであり、内部に図示せぬコントローラを保持している。マイクロプロセッサ１８２において動作するソフトウエアの実行コード、復号関連処理に必要となる各種データ、購入したコンテンツデータの使用権情報などが記憶される。

【０１１６】暗号化処理部１８６は、コンテンツデータおよびメタデータの復号関連処理を行う。暗号化処理部１８６は、さらに、以下の機能を提供するサブブロックにより構成される。

【０１１７】暗号化処理サブブロック１８７は、DES、RSAなどの暗号化アルゴリズムにより暗号化されたコンテンツデータの復号処理を行う。

【０１１８】ディジタル署名検証サブブロック１８８は、DSAなどによるディジタル署名アルゴリズムによりディジタル署名が付加されたコンテンツデータおよびメタデータのディジタル署名検証処理を行う。

【０１１９】ハッシュ値計算サブブロック１８９は、ハッシュ関数による計算を行う。

【０１２０】図１５は、暗号化処理ブロック１６３が、コントローラ１６２等と送受信するデータ形式の例を示す図である。コントローラ１６２は、暗号化処理ブロック１６３に対して、図１５のデータ形式のコマンドデータで処理を要求する。また、暗号化処理ブロック１６３は、コマンドデータに基づいて各ブロックを制御し、所定の処理を実行させるとともに、コマンドデータにより処理を要求したコントローラ１６２に対して、図１５のデータ形式のレスポンスデータで処理結果を送信する。

【０１２１】フィールド１は、データ種識別フィールドであり、コマンドデータ、またはレスポンスデータの種類が記述される。

【０１２２】フィールド２は、データ番号フィールドであり、コマンドデータ、またはレスポンスデータの番号が記述される。

【０１２３】フィールド３は、データ長フィールドであり、データフィールド４に記述されるデータの長さが記述される。

【０１２４】フィールド４は、データフィールドであり、コマンドデータとして処理を要求するデータ、またはレスポンスデータとして送信する処理結果のデータが記述される。以下、コマンドデータ、およびレスポンスデータの例を説明する。

【０１２５】データ番号フィールドに記述される番号が１であるコマンド１は、ディジタル署名の検証処理の要求を表している。フィールド４のデータフィールドに記述されているデータに対して、暗号化処理ブロック１６３は、データが改竄されていないかを検証し、その処理結果をレスポンス１として、データ処理を要求したブロックに送信する。

【０１２６】コマンド２は、ディジタル署名の生成処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されているデータに対して、ディジタル署名を付加したデータをレスポンス２として、データ処理を要求したブロックに送信する。

【０１２７】コマンド３は、暗号化されているデータの復号処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されている暗号化されているデータに対して、復号処理を行い、復号したデータをレスポンス３として、データ処理を要求したブロックに送信する。

【０１２８】コマンド４は、暗号化処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されているデータを暗号化し、暗号化したデータをレスポンス４として、データ処理を要求したブロックに送信する。

【０１２９】コマンド５は、ハッシュ値計算の要求を表している。ハッシュ値計算サブブロック１８９は、フィールド４のデータフィールドに記述されているデータ、およびアルゴリズムをもとに、ハッシュ関数による計算を行い、計算結果のデータをレスポンス５として、データ処理を要求したブロックに送信する。

【０１３０】コマンド６は、処理の停止要求を表している。このコマンドを受信した場合、暗号化処理ブロック１６３は、その時点で行っている処理を停止し、停止した旨の通知をレスポンス６として処理の停止を要求するブロックに送信する。

【０１３１】コマンド７は、使用権情報の送信要求を表している。このコマンドを受信した場合、暗号化処理ブロック１６３は、自らがフラッシュメモリ１８５に保持している使用権情報を暗号化して、決済サーバ５８にレスポンス７として送信する。

【０１３２】コマンド２０は、外部装置または他のブロックから送信されるメッセージである。そのデータフィールドには、コントローラ１６２などからメッセージが入力される。

【０１３３】レスポンス３０は、暗号化処理ブロック１６３が、外部装置または他のブロックに対して送信するメッセージである。

【０１３４】以下、コンテンツプロバイダ５１が提供するコンテンツデータを、利用者５５が利用するまでの一連の処理についてフローチャートを参照して説明する。

【０１３５】始めに、図１６のフローチャートを参照して、コンテンツプロバイダ５１が管理するコンテンツサーバ５２の処理を説明する。

【０１３６】ステップＳ４１において、データキャプチャ装置７１は、ビデオカメラ、およびオーディオレコーダなどから取り込んだアナログデータ、またはディジタルデータを、コンテンツサーバ５２の各装置が処理できるデータ形式に、ディジタル化処理、または圧縮などの処理を行う。

【０１３７】ステップＳ４２において、データ編集装置７２は、データキャプチャ装置７１から取得したデータから、コンテンツプロバイダ５１の指令に基づいて、利用者５５に提供するコンテンツデータを作成する。また、データ編集装置７２は、メタデータ生成装置７３が生成するメタデータをコンテンツデータに付加する。

【０１３８】図１７は、メタデータ生成装置７３が生成するメタデータの例を示す図である。図１７（Ａ）のメタデータ１の例において、フィールド１には、コンテンツプロバイダ５１を特定するコンテンツプロバイダＩＤが２、メタデータ１に対応するコンテンツデータ（以下、適宜、コンテンツデータ１と称する。後述する他のメタデータが付加されるコンテンツデータの場合も同様とする）を特定するコンテンツＩＤが１、コンテンツデータ１の著作権の権利発生日時が西暦２０００年１月１日と記述されている。

【０１３９】フィールド２には、利用者５５によるコンテンツデータ１の利用形態が記述される。ここでは、利

用形態１としてストリーミング、利用形態２として買い取り、および利用形態３として期間限定１年の利用形態が記述されている。ストリーミングによる利用形態は、利用者端末５６において、サービスサーバ５４からコンテンツデータ１を受信しながらリアルタイムで再生する利用形態であり、利用回数が１回のみの利用形態である。買い取りによる利用形態とは、期間および利用回数が無制限である利用形態であり、利用者端末５６に送信されたコンテンツデータ１は、利用者端末５６の図示せぬ記録媒体に記録される。また、期間限定１年の利用形態とは、コンテンツデータ１が利用者端末５６の図示せぬ記録媒体に記録された後、利用者５５は期間が１年間以内であれば、回数は無制限にコンテンツデータ１を利用することが可能な形態である。

【０１４０】フィールド３には、コンテンツデータ１の利用形態毎の料金が記述される。ここでは、コンテンツデータ１を利用形態１のストリーミングにより利用した場合、料金は２０円とされ、コンテンツデータ１を利用形態２の買い取りにより利用した場合、料金は１００円とされ、コンテンツデータ１を利用形態３の期間限定１年の利用形態により利用した場合、料金は５０円とされている。利用者５５は、フィールド３に記述される料金に基づいて、決済センタ５７に対して使用権情報の代金を支払う。

【０１４１】フィールド４には、コンテンツデータ１の形式的な情報が記述される。ここでは、コンテンツデータ１の総データ量は１５０MBで、利用者端末５６のデータ再生装置１５２で再生した場合の再生時間は１０分と記述されている。また、コンテンツデータ１は、MPEG（Moving Picture Experts Group）２の規格で圧縮されているビデオデータであり、データ転送速度は2Mbpsと記述されている。

【０１４２】フィールド５には、データ暗号化装置７４がコンテンツデータおよびメタデータに施した暗号関連処理の情報が記述される。この例で、ディジタル署名の生成アルゴリズムはDSA、コンテンツデータ１の暗号化アルゴリズムはDES、コンテンツデータ１の暗号化のデータ単位は２５６KBと記述されている。暗号化のデータ単位は、１つの暗号化の鍵で連続して暗号化する場合のデータの大きさである。暗号化に利用した鍵はさらに別の鍵（メタ鍵）で暗号化されており、メタ鍵は決済センタ５７に委託され、利用者５５が使用権情報を購入した場合、決済サーバ５８から使用権情報とともに、後述する図２３の使用権情報のデータ形式で、利用者５５に提供される。

【０１４３】フィールド６には、利用者端末５６のSTB１５１に含まれる暗号化処理ブロック１６３が処理するコンテンツデータ１に関する情報が記述される。この例で、暗号化処理ブロック１６３に要求される復号関連処理は、コンテンツデータ１の各暗号化単位ブロック毎に付加されているディジタル署名の検証処理、および暗号化されているコンテンツデータ１の復号処理である。

【０１４４】まず、STB１５１のコントローラ１６２が、暗号化処理ブロック１６３に対して転送するデータの転送周期が記述されている。暗号化処理ブロック１６３が処理するディジタル署名の検証が必要なデータの転送周期は１秒とされ、また、復号処理が必要な暗号化されているコンテンツデータ１の転送周期も１秒とされている。

【０１４５】次に、暗号化処理ブロック１６３が処理する各処理の優先度を示す処理順位が設定されている。ここでは、ディジタル署名の検証の処理順位は２、コンテンツデータ１の復号処理の処理順位は１と設定されている。２つの処理が暗号化処理ブロック１６３に要求された場合、ここで設定されている処理順位により、暗号化処理ブロック１６３はコンテンツデータ１の復号処理を優先して処理することになる。

【０１４６】さらに、フィールド６には、各処理の取扱情報が記述される。取扱情報は、第１の処理より優先度が高い第２の処理があり、第１の処理を実行することができない場合の第１の処理の取り扱い方法についての情報である。この例の場合、ディジタル署名の検証処理より、処理順位が高い（リアルタイム性が高い）第２の処理が存在し、STB１５１の暗号化処理ブロック１６３は、第２の処理が終了し、次の第２の処理が必要なデータが転送されてくるまでの間に、ディジタル署名の検証を行うことができない場合、ディジタル署名の検証処理は、第２の処理が全て終了した後に処理する（遅延処理する）と設定されている。また、暗号化処理ブロック１６３は、遅延処理することをコントローラ１６２に通知するようにも設定されている。

【０１４７】また、暗号化されているコンテンツデータ１の復号処理より、処理順位が高い（リアルタイム性が高い）第２の処理が存在し、STB１５１の暗号化処理ブロック１６３は、第２の処理が終了し、次の第２の処理が必要なデータが転送されてくるまでの間に、コンテンツデータ１の復号処理を行うことができない場合も、ディジタル署名の検証処理と同様に、遅延処理を行い、またコントローラ１６２に通知するように設定されている。

【０１４８】図１７（B）のメタデータ２の例において、フィールド１およびフィールド５に記述されている内容はメタデータ１と同一の内容である。フィールド６に記述されている取扱情報には、ディジタル署名の検証処理より、処理順位が高い（リアルタイム性が高い）第２の処理が存在し、STB１５１の暗号化処理ブロック１６３は、第２の処理が終了し、次のディジタル署名の検証が必要なデータが転送されてくるまでの間に、ディジタル署名の検証を行うことができない場合、ディジタル署名の検証処理は、無視すると設定され、記述されてい

る。

【０１４９】図１６に戻って、ステップS４３において、データ暗号化装置７４は、データ編集装置７２から転送されるコンテンツデータおよびメタデータに暗号関連処理を施す。

【０１５０】すなわち、乱数生成ブロック９４は、暗号化鍵（コンテンツデータ用）として所定のビット数の乱数を生成し、暗号化処理サブブロック９６に供給する。

【０１５１】暗号化処理サブブロック９６は、乱数生成ブロック９４が生成した乱数を暗号鍵としてコンテンツデータを暗号化するとともに、使用権情報に配置されて決済サーバ５８から利用者端末５６に対して送信されるメタ鍵を使用して、暗号化鍵（コンテンツデータ用）をDESなどの共通鍵暗号方式で暗号化する。

【０１５２】ハッシュ値計算サブブロック９８は、コンテンツサーバ５２がサービスプロバイダ５３に対して送信するメタデータにハッシュ関数を適用してハッシュ値を算出する。

【０１５３】ディジタル署名生成サブブロック９７は、ハッシュ値計算サブブロック９８が抽出したハッシュ値を、乱数生成ブロック９４が生成した乱数よりなる暗号化鍵を利用して暗号化し、ディジタル署名を生成する。

【０１５４】ステップS４４において、データ記憶装置７５は、データ暗号化装置７４により暗号関連処理が施されたデータを記憶し、必要に応じてデータ送信装置７６に出力する。

【０１５５】ステップS４５において、データ送信装置７６は、サービスプロバイダ５３が管理するサービスサーバ５４にメタデータおよびコンテンツデータを送信する。

【０１５６】図１８は、ステップS４５の処理により送信されるデータのフォーマットの例を示す。レイヤ１は、ステップS４２の処理により生成されたメタデータ、ステップS４３の処理により付加されたメタデータ用のディジタル署名、ステップS４３の処理で用いられた暗号化鍵（コンテンツデータ用）、並びにコンテンツデータにより構成される。コンテンツデータは、さらに、レイヤ２としての暗号化単位ブロックにより構成されている。暗号化単位ブロックは、コンテンツデータ１、およびコンテンツデータ２の場合、２５６KB毎のブロックとされている。レイヤ２の暗号化単位ブロックはさらに、レイヤ３としての、２５６KBのデータ長のブロックと、ディジタル署名とで構成されている。従って、この例では、この暗号化データに付加されているディジタル署名を検証することにより、コンテンツデータの各暗号化単位ブロックに、改竄などの不正処理が行われているか否かを判断することができる。

【０１５７】次に、図１９のフローチャートを参照して、サービスプロバイダ５３が管理するサービスサーバ５４の処理を説明する。

【０１５８】ステップS６１において、データ送受信装置１１１は、コンテンツサーバ５２から、暗号関連処理が施されたコンテンツデータおよびメタデータを受信する。

【０１５９】ステップS６２において、メタデータ生成装置１１３は、送信されてきたメタデータを確認し、元のデータを変更し、新たなメタデータを生成する。すなわち、このときデータ暗号化装置１１４は、コンテンツプロバイダ５１から決済サーバ５８を介して予め取得したメタ鍵を利用して、送信されてきた暗号化鍵（コンテンツデータ用）（図１８）を復号し、復号した暗号化鍵（コンテンツデータ用）（図１８）を利用してディジタル署名（メタデータ用）（図１８）を復号する。そして、メタデータ生成装置１１３は、復号して得られたメタデータと、平文で送信されてきたメタデータを比較し、両者が一致していること、すなわち、メタデータが改竄されていないことを確認する。

【０１６０】さらに、メタデータ生成装置１１３は新たにメタデータを生成する。このメタデータは、コンテンツサーバ５２が生成したメタデータ１（図１７（A））およびメタデータ２（図１７（B））のフィールド１およびフィールド３の内容を、サービスプロバイダ５３が利用者５５に通知する情報に書き換えたデータである。メタデータ３およびメタデータ４の内容は、サービスプロバイダ５３が決定する。

【０１６１】図２０は、図１７に示されるコンテンツプロバイダ５１が生成したメタデータを、ステップS６２の処理で、メタデータ生成装置１１３が変更して生成したメタデータの例を示す。図１７（A）のメタデータ１を変更して生成されたメタデータ３（図２０（A））の例においては、フィールド１には、サービスプロバイダ５３を特定するサービスプロバイダIDが１、メタデータ３を作成した日時が西暦２０００年１月２日と記述されている。

【０１６２】フィールド３に記述されている料金には、図１７（A）に示すメタデータ１のフィールド３に記述されている料金に、サービスプロバイダ５３が利用者５５に対してコンテンツデータを送信する送信料が付加されている。メタデータ３では、料金は、コンテンツデータをストリーミングの利用形態により利用する場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、サービスプロバイダ５３が受け取る送信料の１０円が付加されて３０円とされ、コンテンツデータを買い取りの利用形態により利用する場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、サービスプロバイダ５３が受け取る送信料の５０円が付加されて１５０円とされ、コンテンツデータを期間限定１年の利用形態により利用する場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、サービスプロバイダ５３が受け取る送信料の３０円が付加さ

れて８０円とされている。

【０１６３】図１７（Ｂ）のメタデータ２を変更して生成された図２０（Ｂ）のメタデータ４の例においても、メタデータ３の場合と同様の変更がメタデータ生成装置１１３によりされている。

【０１６４】ステップＳ６３において、データ暗号化装置１１４は、新たに生成したメタデータのハッシュ値を演算し、それを暗号化鍵（コンテンツデータ用）で暗号化し、新たなディジタル署名を生成し、ステップＳ６２の処理で生成された新たなメタデータに付加する。データ暗号化装置１１４の暗号関連処理は、コンテンツサーバ５２のデータ暗号化装置７４の処理と同様にして行われれる。

【０１６５】ステップＳ６４において、データ編集装置１１２は、サービスサーバ５４の各装置で処理されたデータを編集し、利用者５５に提供するコンテンツデータを作成する。このため、暗号化装置１１４は、送信されてきたコンテンツデータを暗号化鍵（コンテンツデータ用）で一旦復号する。その後データ編集装置１１２により行われる編集には、コンテンツサーバ５２から送信されたコンテンツデータにステップＳ６２の処理で生成されたメタデータを付加する処理、または複数のコンテンツデータを統合し、１つのコンテンツデータにまとめて利用者５５に提供するアルバム化などの処理がある。編集後のコンテンツデータは、データ暗号化装置１１４により暗号化鍵（コンテンツデータ用）を用いて再び暗号化される。

【０１６６】ステップＳ６５において、データ記憶装置１１６は、データ編集装置１１２で編集され、データ暗号化装置１１４により暗号化されたデータを記憶する。

【０１６７】ステップＳ６６において、データ送受信装置１１１は、利用者５５が管理する利用者端末５６から、メタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。その後、データ送受信装置１１１が、メタデータの送信が要求されたと判定した場合、処理はステップＳ６７に進む。

【０１６８】ステップＳ６７において、データ送受信装置１１１は、利用者５５が要求するコンテンツデータに対応するメタデータを、データ記憶装置１１６から取得し、ネットワーク２２を介して利用者端末５６に送信する。データ送受信装置１１１が送信するメタデータを受信した利用者端末５６のSTB１５１は、メタデータに記述されている内容を確認し、コンテンツデータの復号関連処理の準備をする。STB１５１の詳細な処理については後述するが、その後、STB１５１からコンテンツデータの送信が要求されてくる。

【０１６９】そこで、ステップＳ６８において、データ送受信装置１１１は、利用者端末５６からコンテンツデータの送信が要求されたか否かを判定する。

【０１７０】データ送受信装置１１１が、利用者端末５６からコンテンツデータの送信が要求されたと判定した場合、処理はステップＳ６９に進み、データ送受信装置１１１は、データ記憶装置１１６に記憶されているコンテンツデータを、ネットワーク２２を介して利用者端末５６に送信する。

【０１７１】次に、決済センタ５７が管理する決済サーバ５８が、利用者端末５６に対して行うコンテンツデータの使用権情報の発行処理について、図２１および図２２のフローチャートを参照して説明する。

【０１７２】ステップＳ８１において、ライセンス装置１３２は、利用者端末５６からコンテンツデータの使用権情報の購入が要求されたか否かを判定し、要求されたと判定するまで待機する。ライセンス装置１３２が、利用者端末５６から使用権情報の購入が要求されたと判定した場合、処理はステップＳ８２に進む。

【０１７３】ステップＳ８２おいて、ライセンス装置１３２は、使用権情報の購入を要求している利用者５５は、サービスプロバイダ５３からコンテンツデータの提供を受ける契約をしているか否かを確認するため、利用者端末５６のSTB１５１から送信される情報に基づいて、STB１５１は契約対象の機器であるか否かをユーザ管理装置１３３に問い合わせる。この問い合わせに応じて、ユーザ管理装置１３３は、自分自身が管理している契約情報から、使用権情報の購入を要求するSTB１５１は、契約対象の機器であるか否かを検索する。すなわち、このシステムでは、利用者５５はコンテンツデータの提供を受ける前に、サービスプロバイダ５３と予め契約をする必要がある。契約情報は、サービスプロバイダ５３から決済センタ５７に供給され、ユーザ管理装置１３３に登録される。

【０１７４】ステップＳ８３において、ライセンス装置１３２は、ステップＳ８２のユーザ管理装置１３３の検索結果を判定する。ライセンス装置１３２は、使用権情報の購入を要求しているSTB１５１は、契約対象の機器でないと判定した場合、利用者端末５６に対して使用権情報を販売することができないことを通知し、処理を終了する。

【０１７５】ライセンス装置１３２が、使用権情報の購入を要求しているSTB１５１は、契約対象の機器であると判定した場合、処理はステップＳ８４に進み、ライセンス装置１３２は、データ送受信装置１３１からネットワーク２２を介してSTB１５１の暗号化処理ブロック１６３と相互認証を行い、セッション鍵を共有する。

【０１７６】ステップＳ８５において、ライセンス装置１３２は、相互認証が成立したか否かを判定し、相互認証が成立していないと判定した場合、処理を終了する。

【０１７７】ステップＳ８５において、ライセンス装置１３２が、相互認証が成立したと判定した場合、処理はステップＳ８６に進み、ライセンス装置１３２は、STB１

５１から送信される要求内容に基づいて、使用権情報の発行が可能であるか否かを著作権管理装置１３４に問い合わせる。STB１５１から送信される要求内容には、利用者５５が利用を希望するコンテンツデータのコンテンツID、コンテンツデータの利用形態、および使用権情報の代金の決済方法が含まれる。（決済方法がクレジットカードによる決済の場合、クレジットカードのカード番号が、また、決済方法がプリペイドカード型の電子マネーによる決済の場合、プリペイドカードのカード番号が、それぞれ含まれる）このSTB１５１から送信される要求情報は、改竄などの不正処理を防ぐため、暗号化処理ブロック１６３により暗号化されてSTB１５１から送信される。

【０１７８】ステップS８７において、ライセンス装置１３２は、ステップS８６で著作権管理装置１３４に問い合わせた結果を判定する。ライセンス装置１３２は、使用権情報の発行ができないと判定した場合、利用者端末５６に使用権情報の発行ができないことを通知し、処理を終了する。

【０１７９】ステップS８７において、ライセンス装置１３２が、使用権情報の発行が可能であると判定した場合、処理はステップS８８に進み、ライセンス装置１３２は、課金装置１３５に対して課金処理を要求する。

【０１８０】ステップS８９において、課金装置１３５は、自らが管理している料金情報から、利用者５５が要求する使用権情報の代金を取得し、決済装置１３６に対して決済処理の要求をするとともに、利用者端末５６に対して課金情報を通知する。

【０１８１】ステップS９０において、課金装置１３５から決済処理の要求を受けた決済装置１３６は決済処理を行う。決済方法がクレジットカードによる決済の場合、決済装置１３６は、図示せぬクレジットカード会社の決済サーバに、使用権情報の購入を要求している利用者５５のユーザID、および課金装置１３５が取得した使用権情報の代金を通知し、クレジット会社の決済サーバから、決済が可能であるか否かのメッセージを受け取る。決済装置１３６は、メッセージの結果を課金装置１３５に通知する。

【０１８２】利用者５５が要求する決済方法が、プリペイドカード型の電子マネーによる決済の場合、決済装置１３６は、利用者５５から通知されたカードIDと、自分自身が管理するプリペイドカードのカードIDを照合し、決済が可能であるか否かを判定する。決済装置１３６は、この判定結果を課金装置１３５に通知するとともに、決済が可能である場合、利用者５５が使用しているプリペイドカード型の電子マネーの残高情報を更新する。

【０１８３】ステップS９１において、課金装置１３５は、決済装置１３６から通知される情報により、決済が成立したか否かを判定する。決済が成立していないと判定した場合、課金装置１３５は、決済が成立していないことを利用者端末５６に通知し、処理を終了する。

【０１８４】ステップS９１において、課金装置１３５は、決済が成立したと判定した場合、ライセンス装置１３２に決済が成立したことを通知する。

【０１８５】このときステップS９２において、ライセンス装置１３２は、使用権情報をセッション鍵で暗号化し、ネットワーク２２を介して利用者端末５６に送信する。送信された使用権情報は、STB１５１の暗号化処理ブロック１６３によりセッション鍵で復号される。

【０１８６】図２３は、使用権情報の例を示している。この使用権情報の例では、フィールド１には、利用者５５に対してコンテンツデータの使用権情報の発行を許可するコンテンツプロバイダ５１のIDが２、利用が許可されたコンテンツデータのコンテンツIDが１、および使用権の権利発生日時が西暦２０００年１月２日と記述されている。

【０１８７】フィールド２にはコンテンツプロバイダ５１により許可された利用形態がストリーミングであることが記述されており、フィールド３には、そのストリーミングによる利用形態の料金が３０円とされている。

【０１８８】フィールド４には、メタ鍵が配置されている。通常、利用が許可されたコンテンツデータを復号するための鍵（暗号化鍵（コンテンツデータ用）（図１８））は暗号化されており、メタ鍵はその暗号化鍵（コンテンツデータ用）（図１８）を復号して取得するための鍵である。

【０１８９】フィールド５には、使用権情報全体のディジタル署名が付加される。

【０１９０】使用権情報は、STB１５１の暗号化処理ブロック１６３により、そのディジタル署名の検証が行われた後、暗号化処理ブロック１６３の内部に配置されているフラッシュメモリ１８５に記憶される。記憶された使用権情報は、コンテンツデータの復号関連処理において、適宜、利用される。

【０１９１】次に、使用権情報を取得した後のSTB１５１の処理について、図２４乃至図２６のフローチャートを参照して説明する。ここでは、STB１５１がメタデータ３およびコンテンツデータ３を受信して処理する場合について説明する。

【０１９２】ステップS１１１において、STB１５１のコントローラ１６２は、利用者５５からの指令に基づいてサービスサーバ５４に対して、使用権情報を購入したコンテンツデータ３に対応するメタデータ３の送信を要求する。

【０１９３】ステップS１１２において、データ送受信ブロック１６１は、サービスサーバ５４から送信されたメタデータ３を、ネットワーク２２を介して受信する。

【０１９４】ステップS１１２において、データ送受信ブロック１６１が受信したメタデータ３は、コントロー

ラ１６２に転送される。コントローラ１６２は、メタデータ３にはディジタル署名が付加されているため、ディジタル署名の検証が必要であると認識し、メタデータ３を暗号化処理ブロック１６３に転送する。

【０１９５】ステップS１１３において、暗号化処理ブロック１６３のマイクロプロセッサ１８２は、転送されたメタデータ３のディジタル署名を検証し、メタデータ３の正当性を判断する。

【０１９６】すなわち、ハッシュ値計算サブブロック１８９は、平文で送られてきたメタデータ３にハッシュ関数を適用してハッシュ値を演算する。暗号化処理サブブロック１８７は、フラッシュメモリ１８５に記憶されているメタ鍵で暗号化鍵（コンテンツデータ用）を復号し、さらに、暗号化鍵（コンテンツデータ用）でディジタル署名を復号し、そこに含まれるハッシュ値を得る。ディジタル署名検証サブブロック１８８は、ハッシュ値計算サブブロック１８９が、転送されたメタデータ３の全文からハッシュ関数を利用して算出したハッシュ値と、暗号化処理サブブロック１８７により復号されたハッシュ値を比較することにより、ディジタル署名を検証する。なお、ハッシュ値計算サブブロック１８９が利用するハッシュ関数は、コンテンツサーバ５２のハッシュ値計算サブブロック９８や、サービスサーバ５４のデータ暗号化装置１１４が利用するハッシュ関数と同一の関数である。

【０１９７】マイクロプロセッサ１８２は、ディジタル署名検証サブブロック１８８が検証した結果を取得し、不正処理の有無を判定する。

【０１９８】ステップS１１４において、マイクロプロセッサ１８２は、メタデータ３が正常なデータ（改竄されていないデータ）であるか否かを判定し、不正処理を認識した場合（ハッシュ値が一致しない場合）、コントローラ１６２に通知する。コントローラ１６２は、不正処理の存在を利用者５５に通知し、処理を終了する。

【０１９９】ステップS１１４において、マイクロプロセッサ１８２により、メタデータ３が正常なデータであることが確認された場合、処理はステップS１１５に進み、マイクロプロセッサ１８２は、受信したメタデータ３の内容を、決済センタ５７から購入し、フラッシュメモリ１８５に記憶されている使用権情報の内容と比較する。これにより、データ送受信ブロック１６１が受信したメタデータ３は、利用者５５が使用権情報を購入し、サービスサーバ５４に送信を要求するコンテンツデータ３に対応するメタデータであるか否かがマイクロプロセッサ１８２により判定される。

【０２００】ステップS１１６において、ステップS１１５でマイクロプロセッサ１８２が比較した結果がマイクロプロセッサ１８２により判定される。マイクロプロセッサ１８２は、メタデータ３の内容が使用権情報の内容と一致せず、正当性が確認できないと判定した場合、コントローラ１６２に通知する。コントローラ１６２は、利用者５５に対してメタデータ３に不正処理が存在していることを通知し、処理を終了する。

【０２０１】ステップS１１６において、マイクロプロセッサ１８２が、メタデータ３の内容と使用権情報の内容を比較し、メタデータ３の正当性を確認した場合、処理はステップS１１７に進み、マイクロプロセッサ１８２は、メタデータ３に含まれる暗号関連情報を確認し、コンテンツデータ３の復号関連処理の準備をする。

【０２０２】なお、この例の暗号化処理ブロック１６３は、DESのアルゴリズムで暗号化されているコンテンツデータ３を復号し、復号した結果を転送する速度は４Mbpsであり、またDSAのアルゴリズムで作成されているディジタル署名を検証する処理能力は１Mbpsであるとする。

【０２０３】ステップS１１７において、マイクロプロセッサ１８２は、メタデータ３のフィールド６に記述されている内容から、復号関連処理をリストアップする。この例の場合、マイクロプロセッサ１８２は、DSAのアルゴリズムで生成されて、コンテンツデータ３に付加されているディジタル署名の検証処理と、DESのアルゴリズムで暗号化されたコンテンツデータ３の復号処理をリストアップする。

【０２０４】ステップS１１８において、マイクロプロセッサ１８２は、メタデータ３のフィールド６に記述されている内容から、ステップS１１７の処理でマイクロプロセッサ１８２がリストアップしたディジタル署名の検証処理、およびコンテンツデータ３の復号処理は、いずれも処理が要求されるタイミングに周期性があると認識する。また、マイクロプロセッサ１８２は、それぞれの処理の処理順位を確認する。マイクロプロセッサ１８２は、ディジタル署名の検証処理の処理順位は２と、コンテンツデータ３の復号処理の処理順位は１と設定されていることを認識し、コンテンツデータ３の復号処理を最優先処理に選択する。

【０２０５】ステップS１１９において、マイクロプロセッサ１８２は、メタデータ３のフィールド６の記述から、コントローラ１６２がコンテンツデータ３の復号処理をマイクロプロセッサ１８２に対して要求する周期（復号処理が必要なコンテンツデータ３のデータ単位が転送されてくる周期）は１秒であると認識し、その周期を基準周期に設定する（図６のタイム１およびタイム２は１秒となる）。

【０２０６】ステップS１２０において、マイクロプロセッサ１８２から、最優先処理を選択し、基準周期を設定した旨の通知を受けたコントローラ１６２は、サービスサーバ５４に対してコンテンツデータ３の送信を要求する。

【０２０７】ステップS１２１において、データ送受信ブロック１６１は、ネットワーク２２を介してコンテン

ツデータ３を受信する。

【０２０８】ステップＳ１２２において、データ送受信ブロック１６１からコンテンツデータ３の転送を受けたコントローラ１６２は、コンテンツデータ３のうちの復号処理が必要なデータ単位を、基準周期に基づいて暗号化処理ブロック１６３に転送する（図６の最優先処理データ単位１が転送される）。

【０２０９】ステップＳ１２３において、暗号化処理ブロック１６３は、最優先処理を開始し、コンテンツデータ３のデータ単位を復号する。暗号化処理ブロック１６３が復号したコンテンツデータ３は、適宜、データ再生装置１５２に転送される。

【０２１０】暗号化処理ブロック１６３に含まれる暗号化処理サブブロック１８７は、フラッシュメモリ１８５に記憶されている使用権情報からメタ鍵を取得し、メタ鍵を利用して、データ送受信ブロック１６１がコンテンツデータ３とともに受信した暗号化鍵（コンテンツデータ３用）を復号する。

【０２１１】暗号化処理サブブロック１８７は、復号して取得した暗号化鍵（コンテンツデータ３用）を利用して暗号化されているコンテンツデータ３を復号する。

【０２１２】ステップＳ１２４において、マイクロプロセッサ１８２は、復号処理が必要なコンテンツデータ単位以外に、ディジタル署名の検証が必要なデータ単位がコントローラ１６２から転送されていることを認識する。

【０２１３】マイクロプロセッサ１８２がコンテンツデータ３の復号処理を実行していない場合（マイクロプロセッサ１８２が、図６のタイム１－２の状態である場合）、ステップＳ１２５において、マイクロプロセッサ１８２は、ディジタル署名の検証に要する時間を算出する。

【０２１４】始めに、マイクロプロセッサ１８２は、コンテンツデータ３のデータ単位を復号する場合に要する時間を算出する。マイクロプロセッサ１８２は、メタデータ３のフィールド４の記述から、データ再生装置１５２が、コンテンツデータ３を出力するために、暗号化処理ブロック１６３に対して要求するコンテンツデータ３の復号処理結果の転送速度は２Mbpsであると認識する。そこで、マイクロプロセッサ１８２は、DESのアルゴリズムで暗号化されているコンテンツデータを復号する自分自身の能力は４Mbpsであるため、データ再生装置１５２が要求するデータ単位を処理するためには０．５秒の時間が必要であると算出する（図６のタイム１－１、タイム２－１、タイムn－１は０．５秒となる）。

【０２１５】次に、マイクロプロセッサ１８２は、ディジタル署名の検証に要する時間を算出する，マイクロプロセッサ１８２は、DSAのアルゴリズムで生成されているディジタル署名を検証する自分自身の能力は１Mbpsであるため、データ再生装置１５２が要求するデータを処理するためには２秒の時間が必要であると算出する。

【０２１６】ステップＳ１２６において、マイクロプロセッサ１８２が、ステップＳ１２５で算出した結果が判断される。マイクロプロセッサ１８２は、ステップＳ１２５で算出した時間から、次の復号処理が必要なコンテンツデータ３のデータ単位（図６の最優先処理データ単位２）が、コントローラ１６２から転送されてくるまでの間（図６のタイム１－２、タイム２－２）に、ディジタル署名を検証することは不可能と認識する。

【０２１７】ステップＳ１２７において、マイクロプロセッサ１８２は、ディジタル署名の検証をどのように処理するか判断するため、メタデータ３のフィールド６に記述されている取扱情報を確認する。

【０２１８】ステップＳ１２８において、マイクロプロセッサ１８２は、メタデータ３のフィールド６には、ディジタル署名の検証の取扱方法として、コントローラ１６２に対する通知、およびディジタル署名の検証の遅延処理が設定されていると認識する。そこで、マイクロプロセッサ１８２は、コントローラ１８２に対してディジタル署名の検証を、最優先処理であるコンテンツデータ３の全てのデータ単位の復号処理が終了した後に処理することを通知するとともに、ディジタル署名の検証を必要とするデータ単位をフラッシュメモリ１８５に記憶する。

【０２１９】ステップＳ１２９において、マイクロプロセッサ１８２は、復号処理が必要なコンテンツデータ３のデータ単位を全て復号処理したか否かを判定し、復号処理が全て終了したと判定するまで、復号処理を優先して処理する。

【０２２０】ステップＳ１２９において、マイクロプロセッサ１８２は、復号処理が必要なコンテンツデータ３のデータ単位を全て復号処理したと判定した場合、処理は、ステップＳ１３０に進む。

【０２２１】ステップＳ１３０において、マイクロプロセッサ１８２は、フラッシュメモリ１８５に記憶させておいたディジタル署名の検証が必要なデータの処理を行う（図６の遅延処理データを処理する）。

【０２２２】ステップＳ１３２において、マイクロプロセッサ１８２は、ディジタル署名の検証を全て終了したと判定した場合、処理を終了する。

【０２２３】次に、STB１５１が、メタデータ４およびコンテンツデータ４を受信して処理する場合について説明する。

【０２２４】ステップＳ１１１乃至ステップＳ１２７の処理は上述したメタデータ３およびコンテンツデータ３を受信した場合と同様の処理である。

【０２２５】ステップＳ１２８において、マイクロプロセッサ１８２は、メタデータ４のフィールド６には、ディジタル署名の検証の取扱方法として、ディジタル署名の検証が必要なデータが転送されてきた場合であって

も、そのデータを無視すると設定されていると認識し、最後先処理であるコンテンツデータ４の復号を続ける。

【０２２６】その後、マイクロプロセッサ１８２は、コンテンツデータ４の復号が全て終了したと判定した場合、全ての処理を終了する。

【０２２７】ここでは、遅延処理するディジタル署名の検証が必要なデータを、最後先処理が終了するまでフラッシュメモリ１８５に記憶させることとしたが、記憶先なども、メタデータに設定することが可能である。また、コントローラ１６２がディジタル署名の検証を必要とするデータの転送を中止するように予め設定しても良い。

【０２２８】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータや、STB１５１などに、記録媒体からインストールされる。

【０２２９】図２７は、一連の処理を実行するソフトウェアがインストールされるパーソナルコンピュータ２０１の構成例を示している。パーソナルコンピュータ２０１は、CPU(Central Processing Unit)２１１を内蔵している。CPU２１１にはバス２１４を介して、入出力インタフェース２１５が接続されている。入出力インタフェース２１５には、キーボード、マウスなどの入力デバイスよりなる入力部２１６、処理結果としての例えば音声信号を出力する出力部２１７、処理結果としての画像を表示するディスプレイなどよりなる表示部２１８、プログラムや各種データを格納するハードディスクドライブなどよりなる記憶部２１９、LAN(LocalArea Network)やインタネットを介してデータを通信するモデムなどよりなる通信部２２０、および、磁気ディスク２２２（フロッピディスクを含む）、光ディスク２２３（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク２２４（MD(Mini Disc)を含む）、もしくは半導体メモリ２２５などの記録媒体に対してデータを読み書きするドライブ２２１が接続されている。バス２１４には、ROM(Read Only Memory)２１２およびRAM２１３が接続されている。

【０２３０】一連の処理を実行するソフトウェアは、磁気ディスク２２２、光ディスク２２３、光磁気ディスク２２４、および半導体メモリ２２５に格納された状態でパーソナルコンピュータ２０１に供給され、ドライブ２２１によって読み出されて、記憶部２１９に内蔵されるハードディスクドライブにインストールされる。記憶部２１９にインストールされているエージェントプログラムは、入力部２１６に入力されるユーザからのコマンドに対応するCPU２１１の指令によって、記憶部２１９からRAM２１３にロードされて実行される。

【０２３１】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２３２】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２３３】

【発明の効果】以上のように、本発明の情報処理装置、情報処理方法、および記録媒体のプログラムによれば、コンテンツデータの特徴情報から、コンテンツデータのデータ処理の種類毎に設定されている処理順位を認識し、処理順位が上位にある優先処理を、コンテンツデータの他の処理に優先して処理するようにしたので、低コストで、かつ、機能変更が容易な、迅速にデータを処理することができるシステムを実現することが可能になる。

【図面の簡単な説明】

【図１】従来の復号LSIの構成例を示すブロック図である。

【図２】本発明を適用したデータ処理システムの構成例を示すブロック図である。

【図３】データ送信装置の処理を説明するフローチャートである。

【図４】データ受信装置の処理を説明するフローチャートである。

【図５】データ受信装置の処理を説明する図３の続きのフローチャートである。

【図６】復号処理部に転送されてくるデータ単位を説明する図である。

【図７】本発明を適用したコンテンツ配信システムの概念を示す図である。

【図８】コンテンツサーバの構成例を示すブロック図である。

【図９】データ暗号化装置の詳細な構成例を示すブロック図である。

【図１０】サービスサーバの構成例を示すブロック図である。

【図１１】決済サーバの構成例を示すブロック図である。

【図１２】利用者端末の構成例を示すブロック図である。

【図１３】セットトップボックスの構成例を示すブロック図である。

【図１４】暗号化処理ブロックの詳細な構成例を示すブロック図である。

【図１５】暗号化処理ブロックが送受信するデータ形式

の例を示す図である

【図１６】コンテンツサーバの処理を説明するフローチャートである。

【図１７】コンテンツサーバが生成するメタデータの例を示す図である。

【図１８】コンテンツサーバが送信するデータのフォーマットの例を示す図である。

【図１９】サービスプロバイダの処理を説明するフローチャートである。

【図２０】サービスサーバが生成するメタデータの例を示す図である。

【図２１】決済サーバの使用権情報の発行処理を説明するフローチャートである。

【図２２】決済サーバの使用権情報の発行処理を説明する図１９の続きのフローチャートである。

【図２３】使用権情報の例を示す図である。

【図２４】セットトップボックスの処理を説明するフローチャートである。

【図２５】セットトップボックスの処理を説明する図２２の続きのフローチャートである。

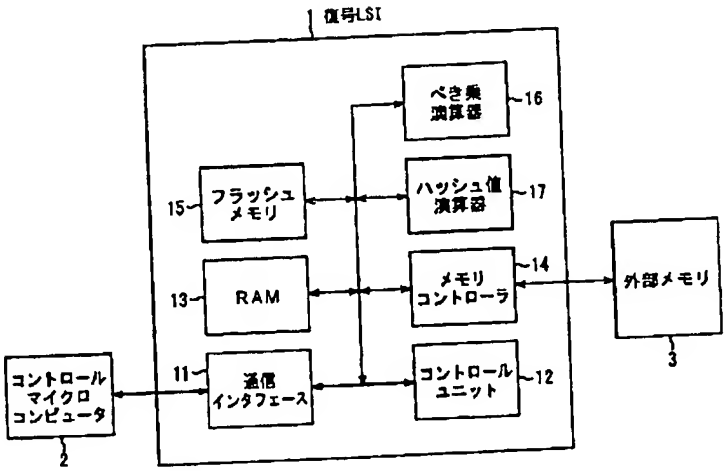
【図２６】セットトップボックスの処理を説明する図２３の続きのフローチャートである。

【図２７】パーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

２１　データ送信装置，　２２　ネットワーク，　２３　データ受信装置，４１　データ受信部，　４２　データ処理判断部，　４３　復号処理部，　４４計算部，　４５　データ記憶部，　５６　利用者端末，　１５１　セットトップボックス，　１５２　データ再生装置，　１６１　データ送受信ブロック，１６２　コントローラ，　１６３　暗号化処理ブロック，　１６４　フラッシュメモリ，　１６５　外部RAM，　１８１　入出力インタフェースブロック，　１８２　マイクロプロセッサ，　１８３　RAM，　１８４　乱数生成ブロック，１８５　フラッシュメモリ，　１８６　暗号化処理部，　１８７　暗号化処理サブブロック，　１８８　ディジタル署名検証サブブロック，　１８９　ハッシュ値計算サブブロック

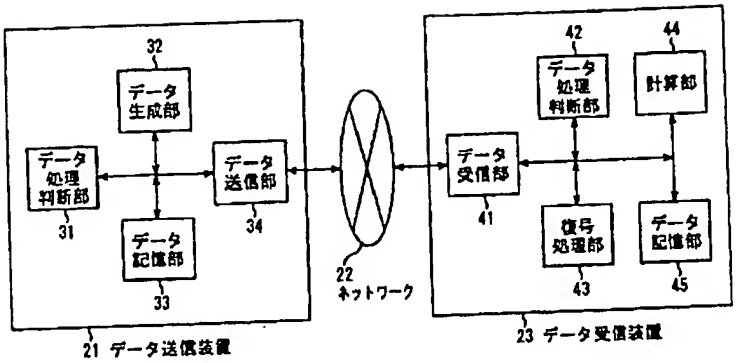
【図１】



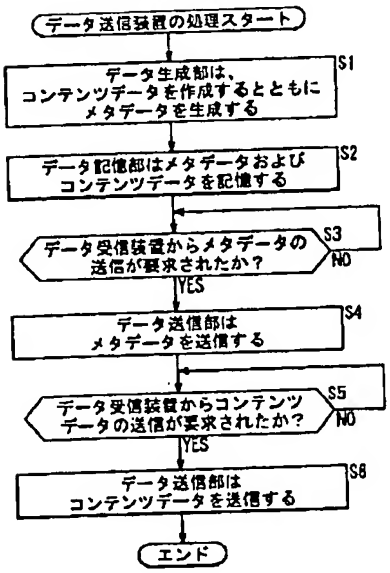
【図１５】

フィールド1	フィールド2	フィールド3	フィールド4
データ種識別フィールド	データ番号フィールド	データ長フィールド	データフィールド

【図２】

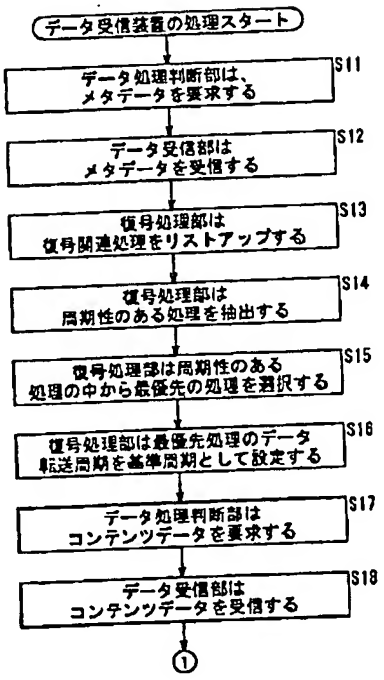

32
データ生成部
データ処理判断部
31
データ送信部
34
データ記憶部
33
21 データ送信装置
22
ネットワーク
42
データ処理判断部
44
計算部
データ受信部
41
復号処理部
43
データ記憶部
45
23 データ受信装置

【図３】

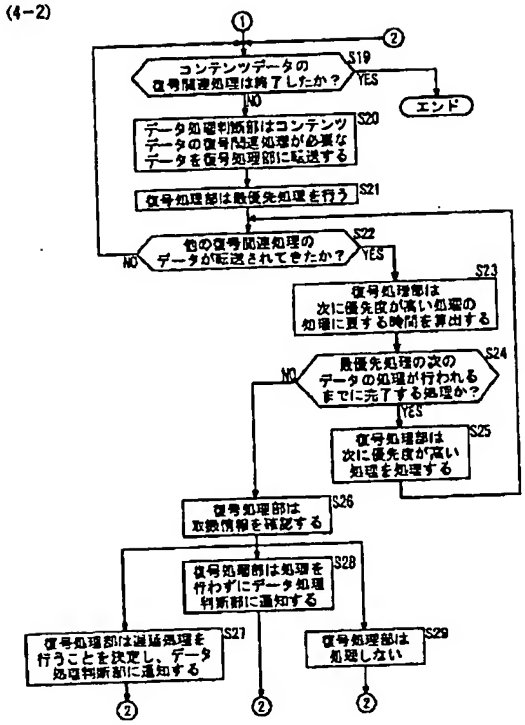

データ送信装置の処理スタート
データ生成部は、コンテンツデータを作成するとともにメタデータを生成する
S1
データ記憶部はメタデータおよびコンテンツデータを記憶する
S2
データ受信装置からメタデータの送信が要求されたか？
S3
NO
YES
データ送信部はメタデータを送信する
S4
データ受信装置からコンテンツデータの送信が要求されたか？
S5
NO
YES
データ送信部はコンテンツデータを送信する
S6
エンド

【図４】

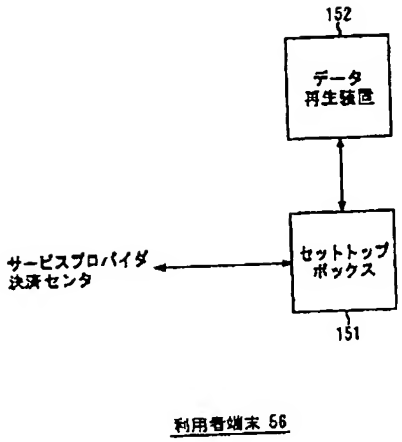
(4-1)


データ受信装置の処理スタート
データ処理判断部は、メタデータを要求する
S11
データ受信部はメタデータを受信する
S12
復号処理部は復号関連処理をリストアップする
S13
復号処理部は周期性のある処理を抽出する
S14
復号処理部は周期性のある処理の中から最優先の処理を選択する
S15
復号処理部は最優先処理のデータ転送周期を基準周期として設定する
S16
データ処理判断部はコンテンツデータを要求する
S17
データ受信部はコンテンツデータを受信する
S18
①

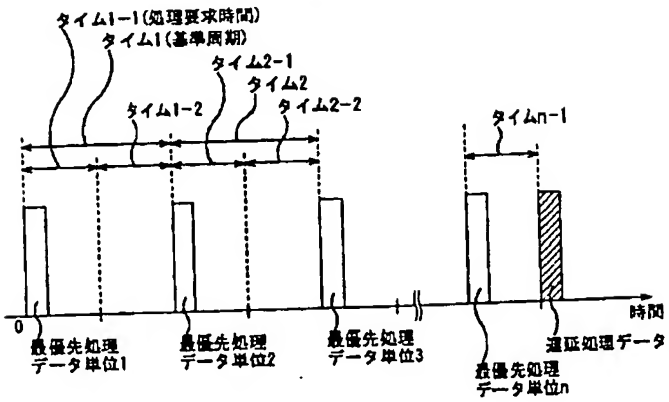
【図５】


(4-2)
①
②
コンテンツデータの復号関連処理は終了したか？
S19
YES
エンド
NO
データ処理判断部はコンテンツデータの復号関連処理が必要なデータを復号処理部に転送する
S20
復号処理部は最優先処理を行う
S21
他の復号関連処理のデータが転送されてきたか？
S22
YES
NO
復号処理部は次に優先度が高い処理の処理に要する時間を算出する
S23
最優先処理の次のデータの処理が行われるまでに完了する処理か？
S24
NO
YES
復号処理部は次に優先度が高い処理を処理する
S25
復号処理部は取扱情報を確認する
S26
復号処理部は処理を行わずにデータ処理判断部に通知する
S28
復号処理部は遅延処理を行うことを決定し、データ処理判断部に通知する
S27
復号処理部は処理しない
S29
②
②
②

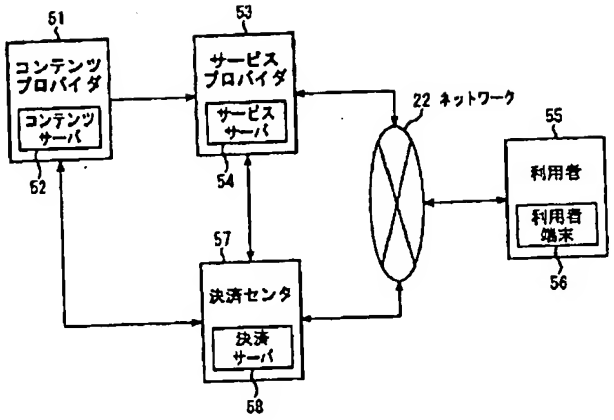
【図１２】


152
データ再生装置
サービスプロバイダ決済センタ
セットトップボックス
151
利用者端末 56

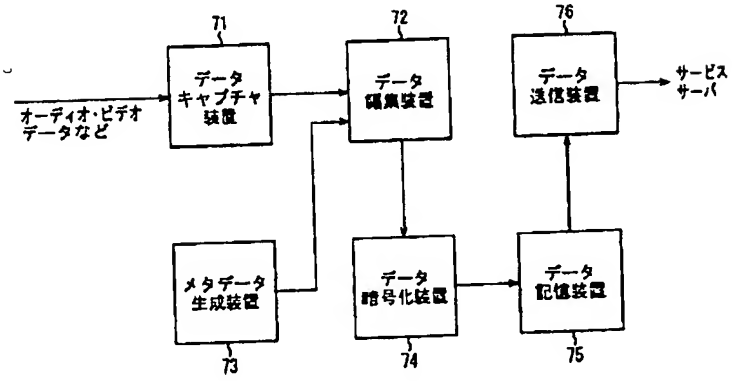
【図６】


タイム1-1(処理要求時間)
タイム1(基準周期)
タイム2-1
タイム2
タイム1-2
タイム2-2
タイムn-1
0
時間
最優先処理データ単位1
最優先処理データ単位2
最優先処理データ単位3
最優先処理データ単位n
遅延処理データ

【図７】



【図８】



コンテンツサーバ 52

【図１７】

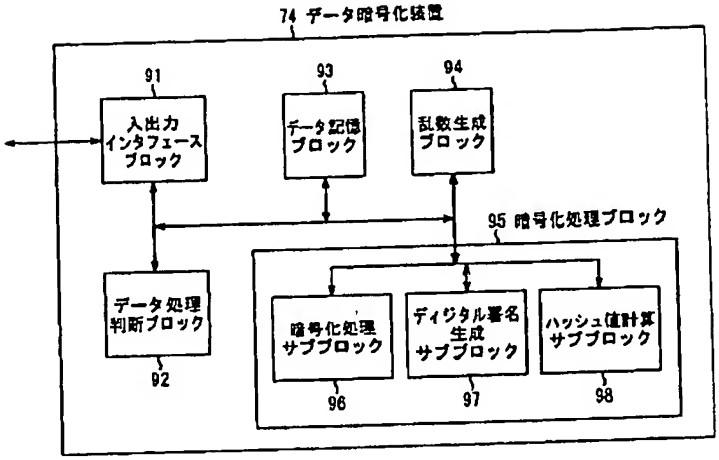
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6			
						転送周期	優先度	取扱
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年1月1日	1 ストリーミング 2 買い取り 3 課題選定1号	1 V320 2 V100 3 V50	再生時間 10分 総データ量 150MB データ形式 MPEG2 ビデオデータ 転送速度 2Mbps	ディジタル署名 DSA 暗号化 DES データ単位 256KB	署名鍵数 (DSA)	1sec	2	追加 通信禁止
					鍵号 (DES)	1sec	1	追加 通信禁止

(A) メタデータ1

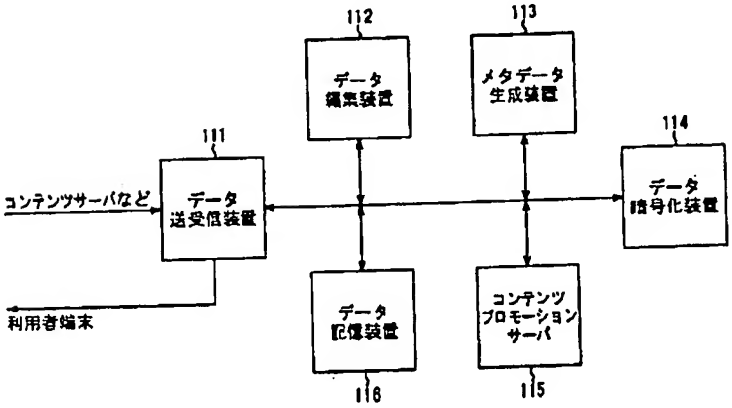
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6			
						転送周期	優先度	取扱
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年1月1日	1 ストリーミング 2 買い取り 3 課題選定1号	1 V320 2 V100 3 V50	再生時間 10分 総データ量 150MB データ形式 MPEG2 ビデオデータ 転送速度 2Mbps	ディジタル署名 DSA 暗号化 DES データ単位 256KB	署名鍵数 (DSA)	1sec	2	取扱
					鍵号 (DES)	1sec	1	取扱 通信禁止

(B) メタデータ2

【図９】



【図１０】

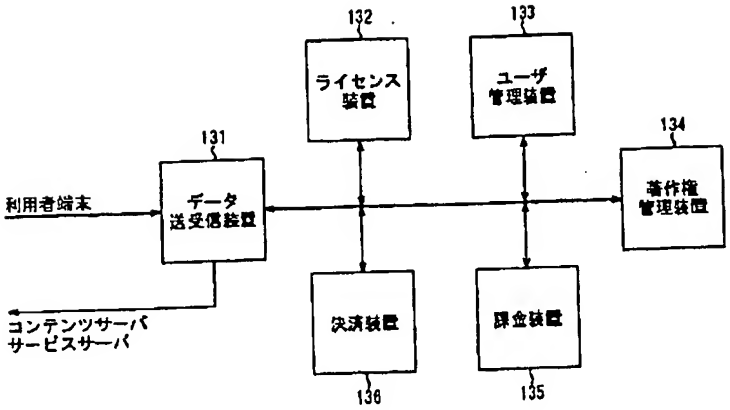


サービスサーバ 54

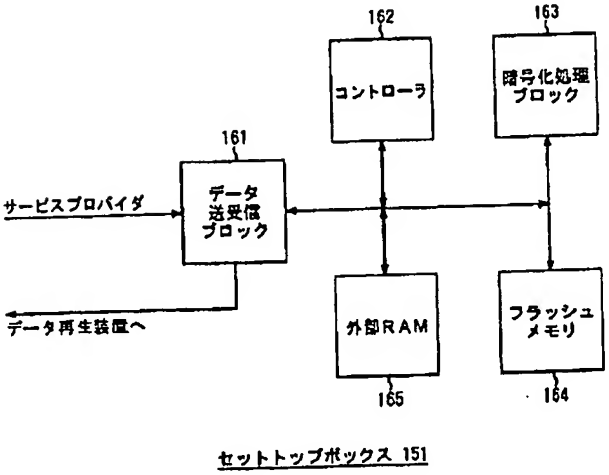
【図２３】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年1月2日	1 ストリーミング	1 ¥30	メタ値	ディジタル署名

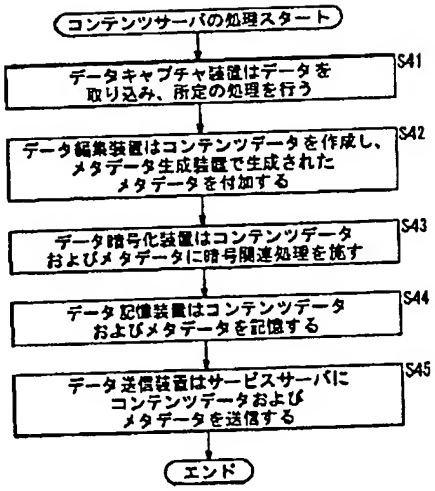
【図１１】


132
ライセンス装置
133
ユーザ管理装置
131
データ送受信装置
134
著作権管理装置
利用者端末
コンテンツサーバ
サービスサーバ
決済装置
136
課金装置
135
決済サーバ 58

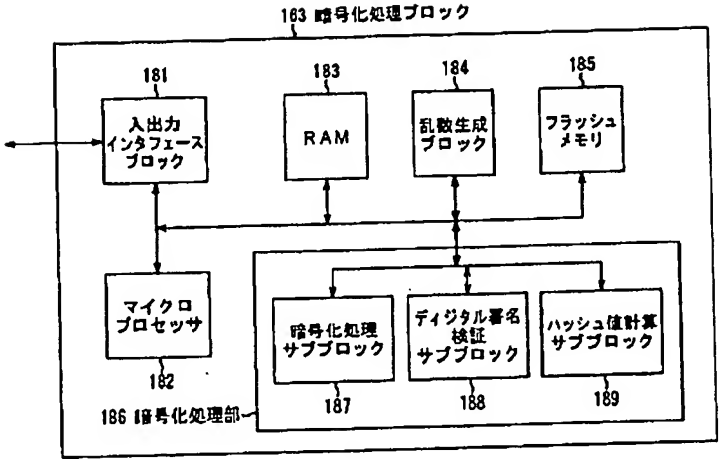
【図１３】


162
コントローラ
163
暗号化処理ブロック
161
データ送受信ブロック
サービスプロバイダ
データ再生装置へ
外部RAM
165
フラッシュメモリ
164
セットトップボックス 151

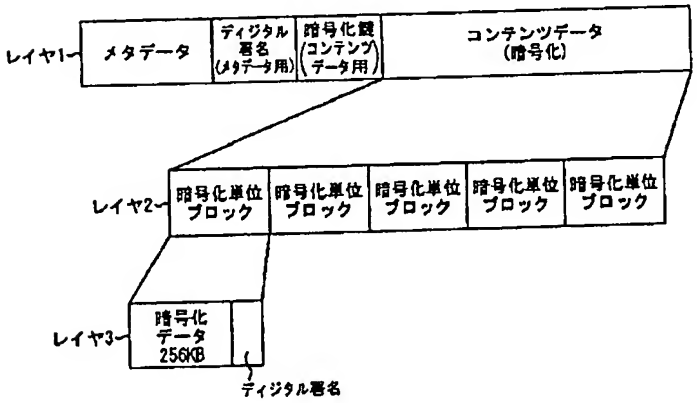
【図１６】


コンテンツサーバの処理スタート
データキャプチャ装置はデータを取り込み、所定の処理を行う
S41
データ編集装置はコンテンツデータを作成し、メタデータ生成装置で生成されたメタデータを付加する
S42
データ暗号化装置はコンテンツデータおよびメタデータに暗号関連処理を施す
S43
データ記憶装置はコンテンツデータおよびメタデータを記憶する
S44
データ送信装置はサービスサーバにコンテンツデータおよびメタデータを送信する
S45
エンド

【図１４】



【図１８】



【図２０】

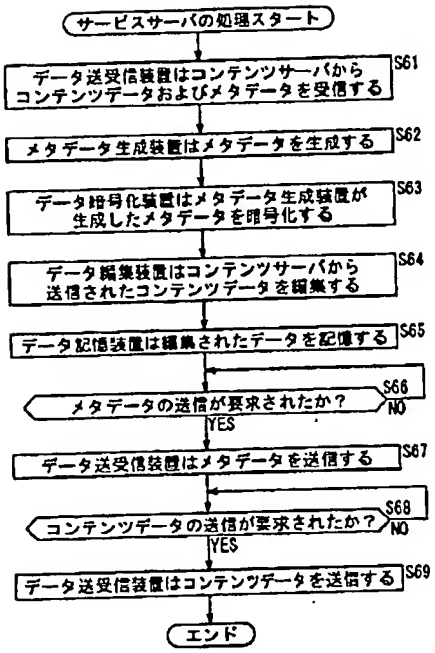
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
サービスプロバイダID 1 コンテンツID 1 メタデータ作成日時 2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 X00 2 Y150 3 Y400	再生時間 10分 総データ量 150MB データ形式 MPEG2 ビデオデータ 転送速度 2Mbps	ディジタル署名 DSA 暗号化 DES データ単位 256KB	転送範囲 優先度 取扱 署名検証 (DSA) 1sec 2 許可 認証局 暗号 (DES) 1sec 1 許可 認証局

(A) メタデータ3

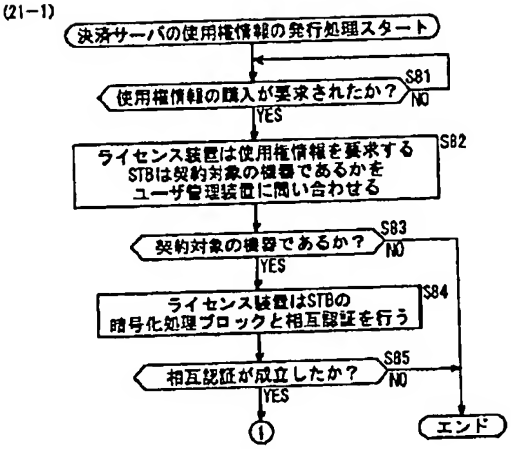
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5	フィールド6
サービスプロバイダID 1 コンテンツID 1 メタデータ作成日時 2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 X00 2 Y150 3 Y400	再生時間 10分 総データ量 150MB データ形式 MPEG2 ビデオデータ 転送速度 2Mbps	ディジタル署名 DSA 暗号化 DES データ単位 256KB	転送範囲 優先度 取扱 署名検証 (DSA) 1sec 2 許可 暗号 (DES) 1sec 1 許可 認証局

(B) メタデータ4

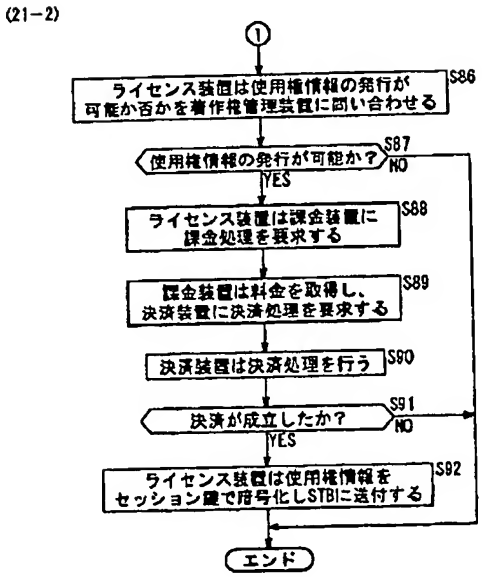
【図１９】



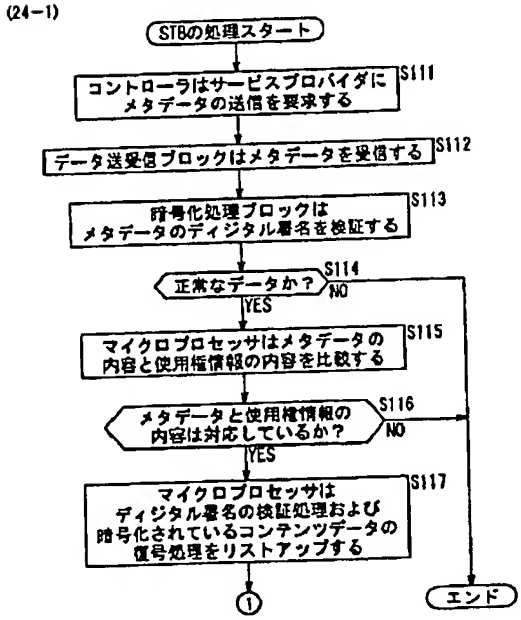
【図２１】



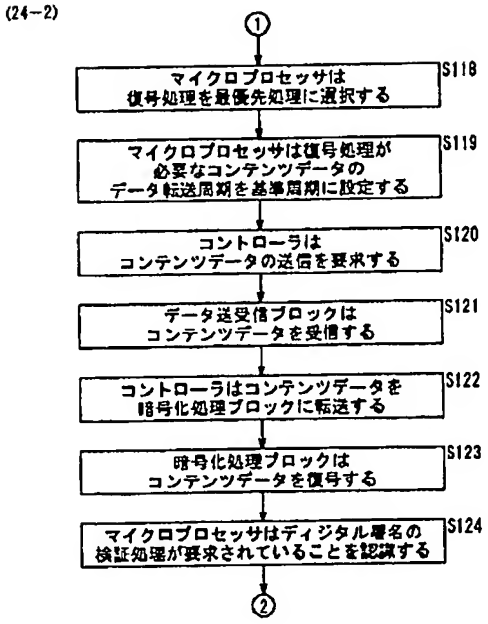
【図２２】



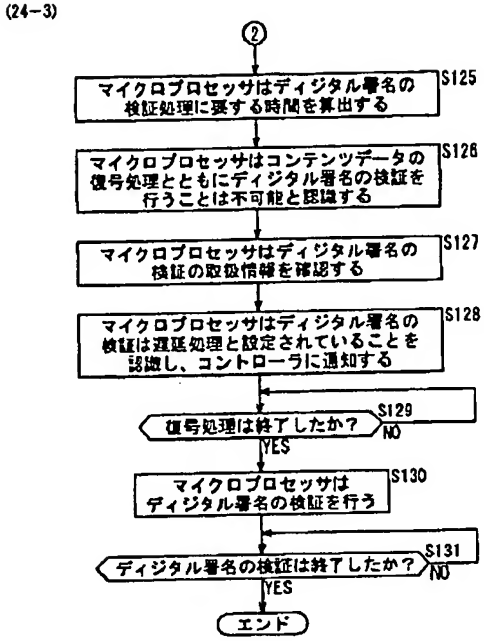
【図２４】



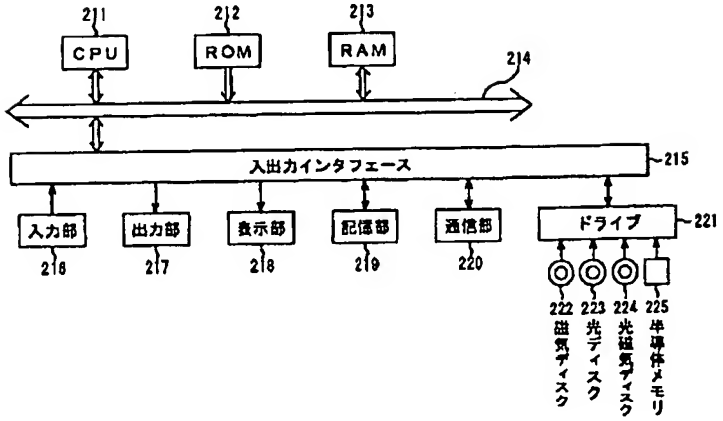
【図２５】



【図２６】



【図２７】



パーソナルコンピュータ 201